WIRELESS 300N OUTDOOR POE ACCESS POINT HANDBUCH

MODELL 524711



INTELLINET™

NETWORK SOLUTIONS

INT-524711-UM-1209-02

Federal Communications Commission (FCC) Konformitätserklärung

FCC Abschnitt 15

Dieses Gerät wurde geprüft und entspricht den Bestimmungen für ein digitales Gerät der Klasse B gemäß Teil 15 der FCC-Bestimmungen. Diese Grenzwerte bieten angemessenen Schutz vor schädlichen Störungen beim Betrieb des Geräts in Wohngebieten.

Dieses Gerät erzeugt und verwendet Hochfrequenzenergie und strahlt sie ab. Wenn es nicht gemäß der Anleitung installiert wird, kann es Interferenzen verursachen. Es wird jedoch keinerlei Garantie übernommen, dass diese bei einer bestimmten Installation nicht auftreten.

Falls dieses Gerät den Radio- und Fernsehempfang stört, was sich durch Ein- und Ausschalten des Geräts nachprüfen lässt, sollten Sie die Störungen durch eine oder mehrere der folgenden Maßnahmen beheben:

1) die Empfangsantenne verlegen oder anders ausrichten

2) den Abstand zwischen Gerät und Empfänger vergrößern

3) das Gerät an eine Steckdose eines Schaltkreises anschließen, der nicht mit dem Empfangsgerät verbunden ist

4) an einen Händler oder erfahrenen Techniker wenden

FCC-Hinweise

Dieses Gerät muss entsprechend der vorgegebenen Anweisungen installiert und betrieben werden. Mindestens 20 cm Abstand müssen während des Wireless Betriebs zwischen Antenne und Körper des Nutzers eingehalten werden.

Dieses Gerät entspricht den Anforderungen von Abschnitt 15 der FCC-Bestimmungen. Für den Betrieb gelten die folgenden zwei Bedingungen: (1) dieses Gerät darf keine schädlichen Interferenzen verursachen; (2) dieses Gerät muss jede empfangene Störung tolerieren, auch solche Störungen, die unerwünschte Funktionen verursachen können.

Bei Änderungen oder Umbauten, die nicht ausdrücklich von der für die Konformität verantwortlichen Partei genehmigt wurden, kann der Benutzer die Berechtigung zum Betrieb des Geräts verlieren.

FCC-Erklärung zur Strahlenbelastung

Diese Geräte entsprechen den von der FCC festgelegten Grenzwerten für die Strahlenbelastung in einer nicht kontrollierten Umgebung. Bei der Installation und Verwendung dieser Geräte sollte ein Abstand von mindestens 20 cm zwischen der Strahlungsquelle und Ihrem Körper eingehalten werden.

Dieser Sender darf nicht in der Nähe von oder in Verbindung mit Antennen oder anderen Sendern betrieben werden.

R&TTE-Konformitätserklärung

Diese Anlage entspricht allen Anforderungen der Richtlinie 1999/5/EG des Europäischen Parlaments und des Rates vom 09. März 1999 über Funkanlagen und Telekommunikationsendeinrichtungen und die gegenseitige Anerkennung ihrer Konfor-mität (R&TTE).

Die R&TTE-Richtlinie ersetzt seit dem 08. April 2000 die Richtlinie 98/13/EEC und hebt diese auf.

Sicherheit

Dieses Gerät wurde unter Beachtung strengster Sicherheitsstandards entwickelt, um die Sicherheit für seine Anwender zu gewährleisten. Dennoch muss beim Umgang mit elektrischen Geräten immer auf mögliche Gefahren durch Stromschlag und Reibungselektrizität geachtet werden. Alle entsprechenden Richtlinien sowie die Richtlinien mit Computergeräten müssen daher bei der Nutzung berücksichtigt werden.

Für die Nutzung in folgenden EU-Ländern vorgesehen

Die ETSI-Version (European Telecommunications Standards Institute - Europäisches Institut für Telekommunikationsnormen) dieses Geräts ist für die Nutzung in folgenden Ländern vorgesehen: Österreich, Belgien, Dänemark, Finnland, Frankreich, Deutschland, Griechenland, Irland, Italien, Luxemburg, Niederland, Portugal, Spanien, Schweden und das Vereinigte Königreich.

Die ETSI-Version dieses Geräts ist außerdem für die Nutzung in folgenden EFTA-Mitgliedsstaaten zugelassen: Island, Liechtenstein, Norwegen und Schweiz.

Für die Nutzung in folgenden EU-Ländern nicht vorgesehen:
Keine.

Inhaltsverzeichnis

Abschnitt 1: Produktinformationen

1-1 Einleitung

Vielen Dank für den Kauf des INTELLINET NETWORK SOLUTIONS™ Wireless 300N Outdoor PoE Access Points, Modell 524711. Er dient mehreren Zwecken - als Access Point für Ihr WLAN, als Bridge für Point-to-Point Verbindungen oder WDS sowie als RADIUS Authentication Server - und vereint alle Funktionen in einem Gerät für eine High-Speed Internetverbindung.

Produkteigenschaften:

- Bis zu 300 Mbit/s Übertragungsgeschwindigkeit
- Kompatibel zum 2,4 GHz IEEE 802.11n Draft 2 Standard, abwärtskompatibel zu IEEE 802.11g/b Standards
- Gehäuse mit Schutzklasse IP67 für optimalen Schutz vor Schmutz und Wasser
- Widersteht Windgeschwindigkeiten bis zu 120 km/h
- 2T2R MIMO Technologie für verbesserten Datendurchsatz und erhöhte Funkabdeckung
- Unterstützt Wi-Fi Protected Setup (WPS) sowie WEP und WPA/WPA2 (TKIP und AES) Datenverschlüsselung
- Unterstützt WMM für Multimedia-Bandbreite
- DHCP-Server vergibt IP-Adressen an alle LAN-Nutzer
- Unterstützte Betriebsmodi: Access Point, Bridge Point-to-Point, Bridge Point-to-Multi-Point, WDS und Universal Repeater
- Einfache Installation über Web-Benutzeroberfläche
- Firmware aktualisierbar
- DHCP
- 3 Jahre Garantie

1-2 Sicherheitshinweise

Zu Ihrer persönlichen Sicherheit und für die Sicherheit des Gerätes, befolgen Sie bitte folgende Hinweise:

1. Entfernen Sie angeschlossene Kabel NICHT MIT GEWALT, trennen Sie zunächst die Verbindung am Access Point.
2. Sollten Sie diesen Acces Point erhöht aufstellen oder an einer Wand hängend anbringen wollen, vergewissern Sie sich, dass er ausreichend gesichert ist, um Schäden an Personen und am Gerät zu vermeiden.
3. Einige Teile dieses Access Points, wie die Antenne (kleinteilig, Verschluckgefahr) und das Netzteil, können für kleine Kinder eine Gefahr darstellen. Um Verletzungen zu vermeiden, stellen Sie den Access Point nicht in Reichweite von Kindern auf!
4. Der Access Point erhitzt sich bei längerer Nutzung ***(dies ist normal und keine Fehlfunktion).*** Stellen Sie den Access Point abseits von Papier, Kleidung, oder anderem brennbarem Material auf.
5. Dieser Access Point ist nicht zur Eigenreparatur geeignet. Sollte er nicht ordnungsgemäß funktionieren, wenden Sie sich bitte an Ihren Händler (bei dem Sie den Access Point erworben haben). ÖFFNEN SIE DEN ACCESS POINT NICHT, sonst verlieren Sie Ihren Garantieanspruch.
6. Lassen Sie den Access Point NICHT MIT FLÜSSIGKEITEN in Berührung kommen. Sollte dies geschehen, berühren Sie ihn nicht, sondern trennen Sie umgehend das Netzteil vom Stromnetz, sofern gefahrlos möglich, oder wenden Sie sich an einen Techniker.
7. Sollten Sie einen befremdlichen Geruch oder gar Rauch am Access Point oder Netzteil wahrnehmen, trennen Sie umgehend das Netzteil vom Stromnetz, sofern gefahrlos möglich, oder wenden Sie sich an einen Techniker.

1-3 Systemvoraussetzungen

- Computer oder netzwerkfähiges Gerät mit Netzwerkkarte (LAN oder WLAN)
- Internetbrowser (Microsoft Internet Explorer 4.0 oder höher, Netscape Navigator 4.7 oder höher, Opera oder Safari).
- Freie Steckdose (100 – 240V, 50/60Hz)

1-4 Lieferumfang

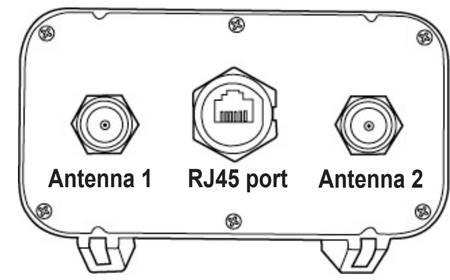
Bevor Sie diesen Access Point das erste Mal nutzen, überprüfen Sie die Packung auf Vollständigkeit und wenden Sie sich ggf. an Ihren Händler.

- Wireless 300N Outdoor PoE Access Point
- 2 abnehmbare Antennen
- Kurzanleitung
- Handbuch auf CD
- Netzteil
- Ethernet Cat5 RJ45 Kabel: 1 m

Abschnitt 2: System- und Netzwerkeinstellungen

2-1 Anschluss der Hardware

Folgen Sie diesen Anweisungen, um die Netzwerkverbindung zwischen dem Wireless Access Point und den Netzwerkgeräten Ihres Computers herzustellen:

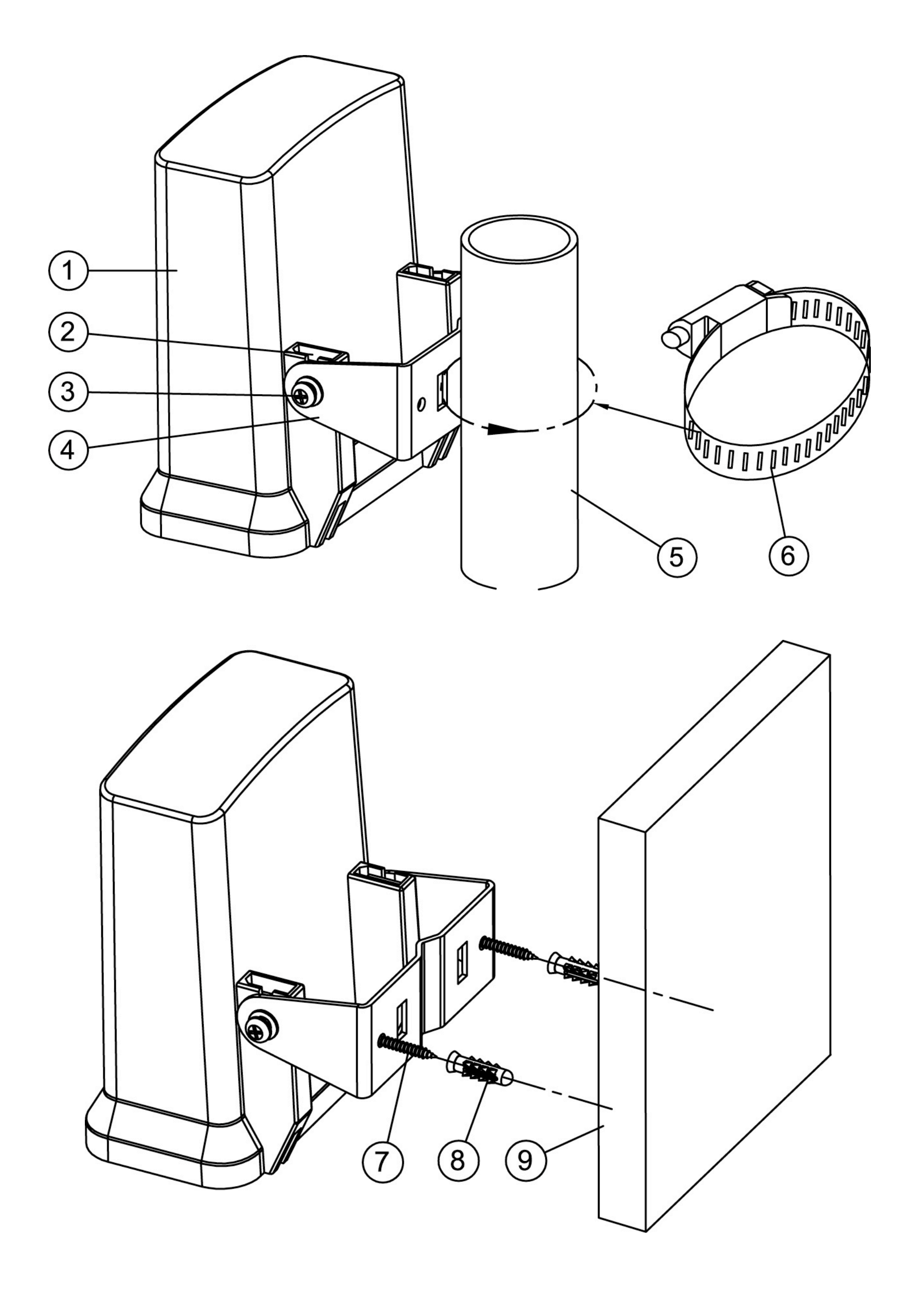


1. Befestigen Sie die Antennen am Access Point. ***HINWEIS:*** Antenne 1 ist die primäre Antenne, die im 11b/g/n-Modus (einzelne Antenne) sendet/empfängt.
2. Mit dem mitgelieferten Ethernet-Kabel verbinden Sie den RJ45-Port des Access Points mit dem „Power/Data Out“-Port des DC-Injektors.
3. Verbinden Sie den LAN-Port am DC-Injektor mit Ihrem Netz werk-Switch oder -Hub.
4. Verbinden Sie das Netzteil mit dem DC-Injektor.
5. Mit dem mitgelieferten Stromkabel verbinden Sie das Netzteil mit einer Steckdose ***HINWEIS:*** Nutzen Sie nur das beiliegende Netzteil für diesen Access Point — nicht das eines anderen Geräts. (Alternativ siehe Schritt 6:)

6. Als Alternative zum mitgelieferten Injektor und Netzteil, können Sie jeden IEEE802.3af-kompatiblen PoE-Injektor verwenden.

Die folgenden Gegenstände werden für die Montage an einem Mast oder an einer Wand benötigt.

1. Access Point
2. Vierkantmuttern (2)
3. M 5-12 Schrauben (2)
4. M-förmige Halterung
5. Mast
6. Schlauchklemme
7. Wandschrauben (2)
8. Wandanker (2)
9. Wand



2-2 Verbindung zum Wireless Access Point per Internetbrowser

Nachdem die Netzwerkverbindung hersgestellt wurde, ist der nächste Schritt die korrekten Netzwerkeinstellungen, damit der Access Point in Ihrer Netzwerkumgebung funktioniert.

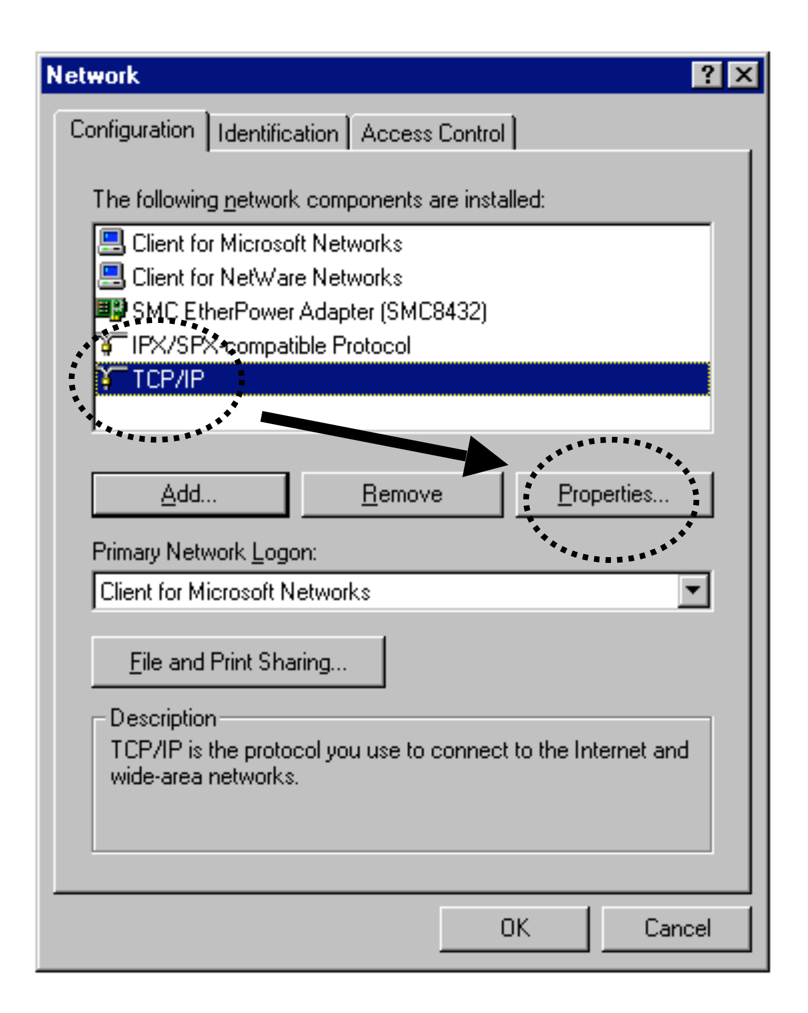
Bevor Sie eine Verbindung zum Access Point herstellen und diesen konfigurieren können, muss Ihr Computer eine IP-Adresse automatisch beziehen können (eine dynamische IP-Adresse). Wenn er eine feste („statische“) IP-Adresse verwendet oder Sie sich unsicher sind, folgen Sie den unten stehenden Anweisungen, um Ihren Computer zur Verwendung einer dynamischen IP-Adresse zu konfigurieren:

Nutzen Sie auf Ihrem Computer das Betriebssystem….

Windows 95/98/Me	**- lesen Sie Abschnitt 2-2-1**
Windows 2000	**- lesen Sie Abschnitt 2-2-2**
Windows XP	**- lesen Sie Abschnitt 2-2-3**
Windows Vista	**- lesen Sie Abschnitt 2-2-4**

2-2-1 Windows 95/98/Me IP-Adresseneinstellungen

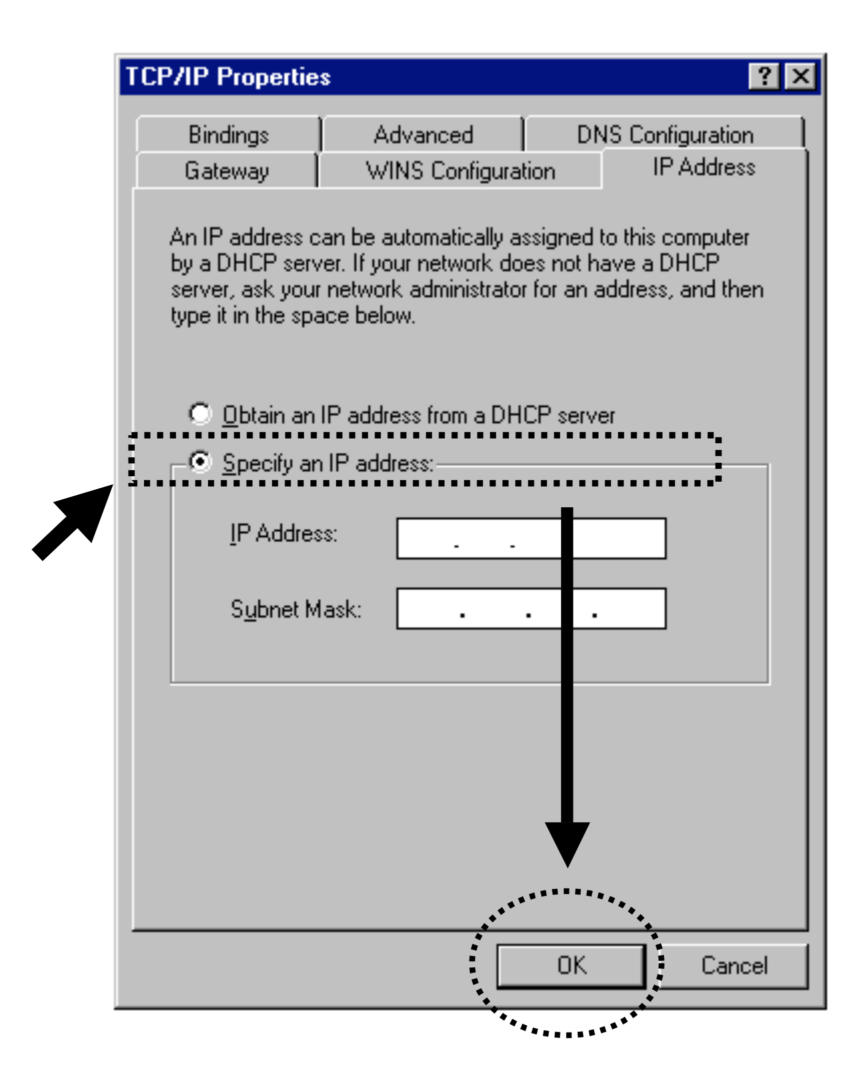
1. Klicken Sie in der linken unteren Ecke Ihres Desktops auf „Start“, dann auf „Systemsteuerung“. Nach einem Doppelklick auf ***„Netzwerk“***, öffnet sich das entsprechende Fenster. Wählen Sie „TCP/IP“ aus, dann klicken Sie auf „Eigenschaften“.



2. Wählen Sie “Eine IP-Adresse festlegen” und geben Sie dann die folgenden Werte in die entsprechenden Felder ein:

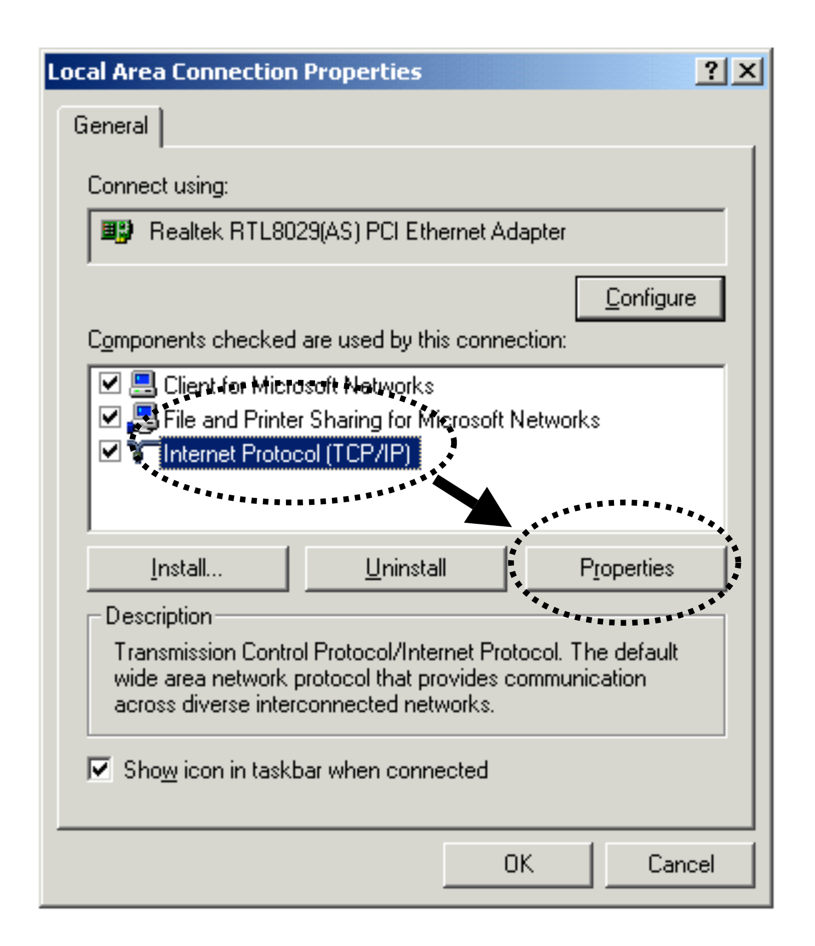
   IP-Adresse: 192.168.2.2
   Subnetzmaske: 255.255.255.0

   Anschließend klicken Sie auf “OK”.



2-2-2 Windows 2000 IP-Adresseneinstellungen

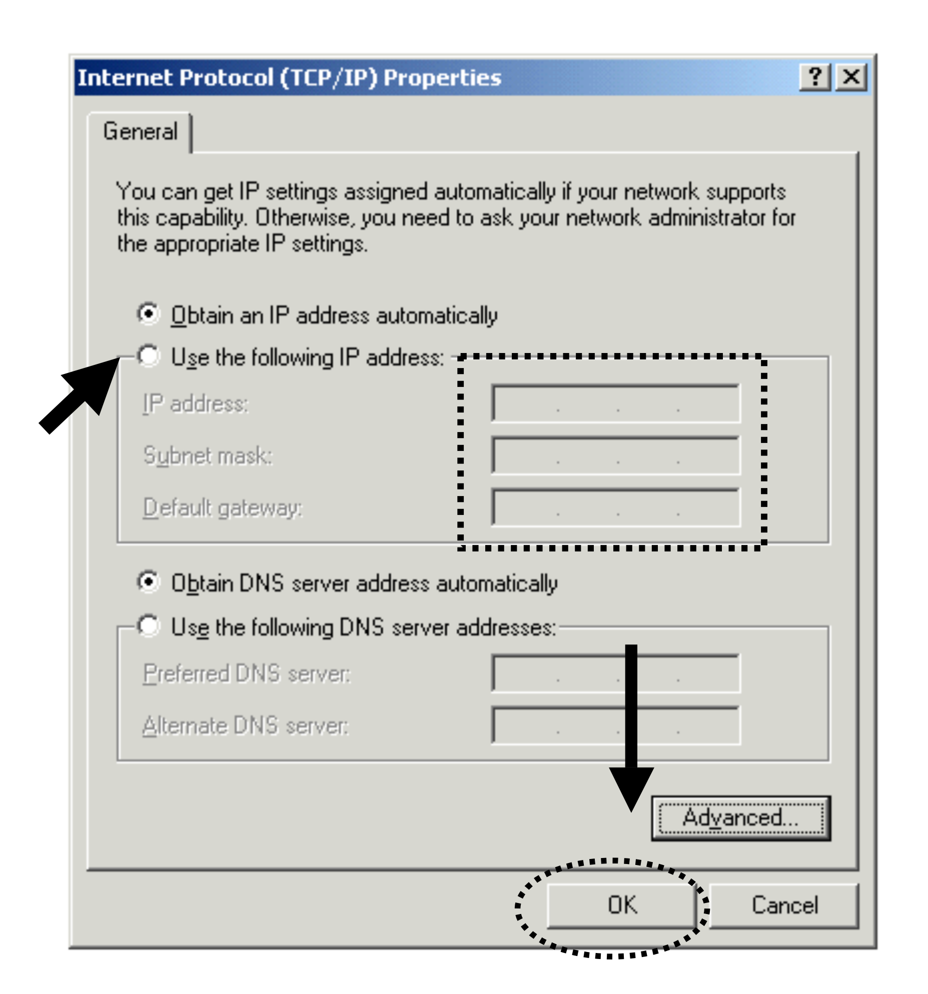
1. Klicken Sie auf Ihrem Desktop unten links auf „Start“, dann auf „Systemsteuerung“. Nach einem Doppelklick auf „***Netzwerk- und DialUp-Verbindungen”,*** klicken Sie auf Lokale Netz-werkverbindung**,** das entsprechende Eigenschaften-Fenster öffnet sich. Wählen Sie „Internetprotokoll (TCP/IP)“ und dann „Eigenschaften“.



2. Wählen Sie “Folgende IP-Adresse verwenden” und geben Sie dann die folgenden Werte in die entsprechenden Felder ein:

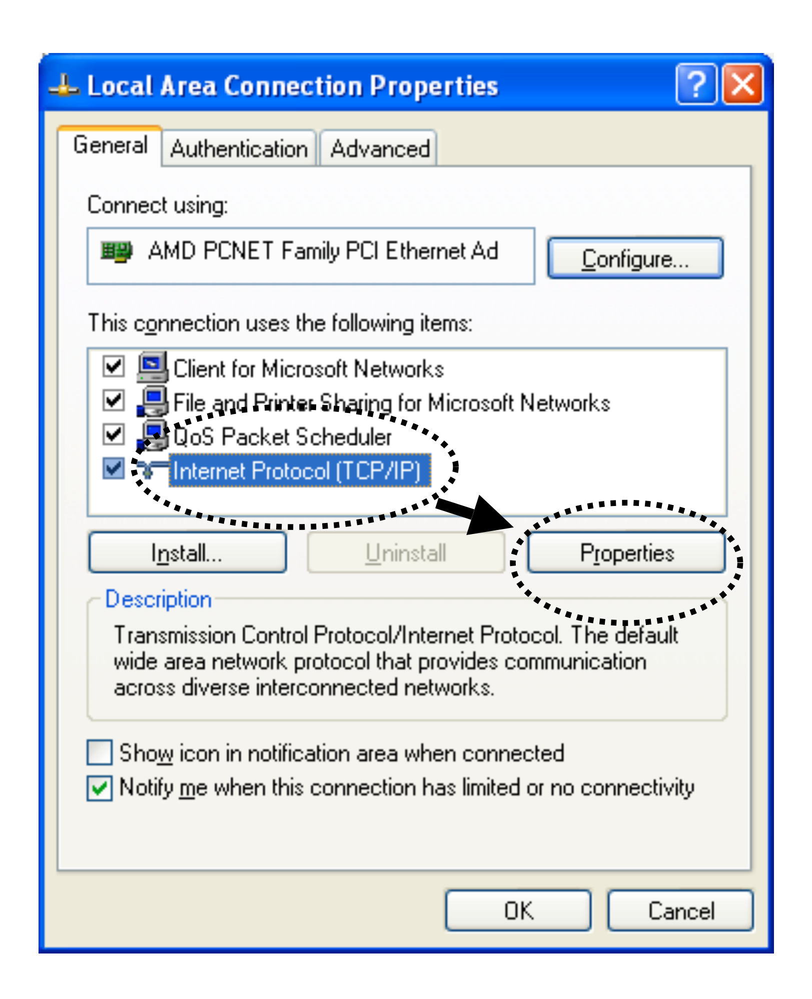
   IP-Adresse: 192.168.2.2
   Subnetzmaske: 255.255.255.0

   Anschließend klicken Sie auf “OK”.



2-2-3 Windows XP IP-Adresseneinstellungen

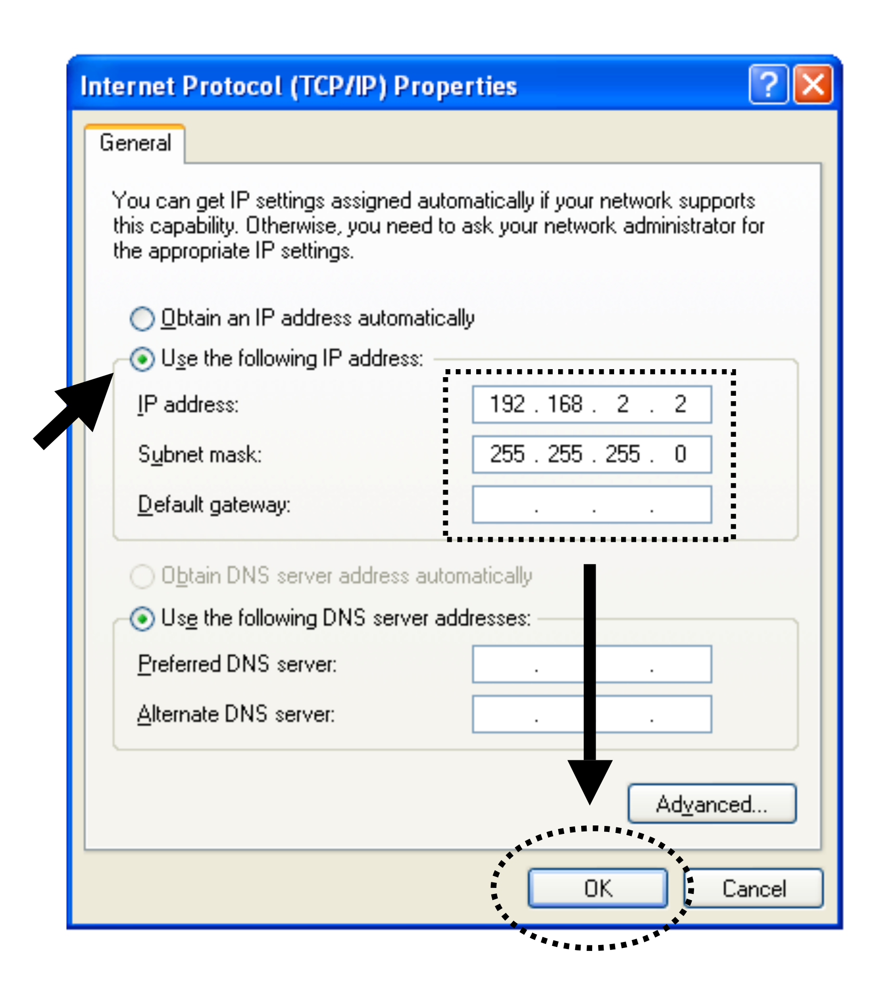
1. Klicken Sie auf Ihrem Desktop unten links auf „Start“, dann auf „Systemsteuerung“. Nach einem Doppelklick auf ***Netzwerk- und Internetverbindungen***, klicken Sie ***Netzwerkverbindung,*** dann doppelklicken Sie auf ***LAN-Verbindung***. Das Fenster ***Status von LAN-Verbindung*** öffnet sich. Klicken Sie auf „Eigenschaften”.



2. Wählen Sie „Folgende IP-Adresse verwenden” und geben Sie dann die folgenden Werte in die entsprechenden Felder ein:

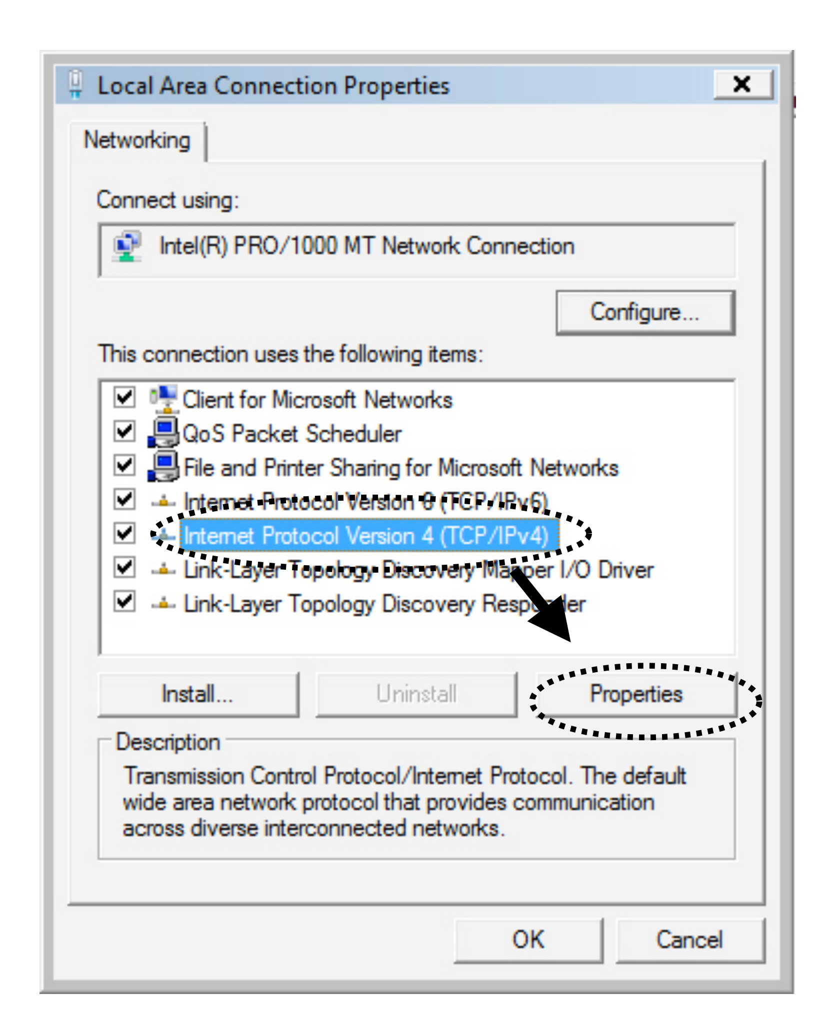
   IP-Adresse: 192.168.2.2
   Subnetzmaske: 255.255.255.0

   Anschließend klicken Sie auf “OK”.



2-2-4 Windows Vista IP-Adresseneinstellungen

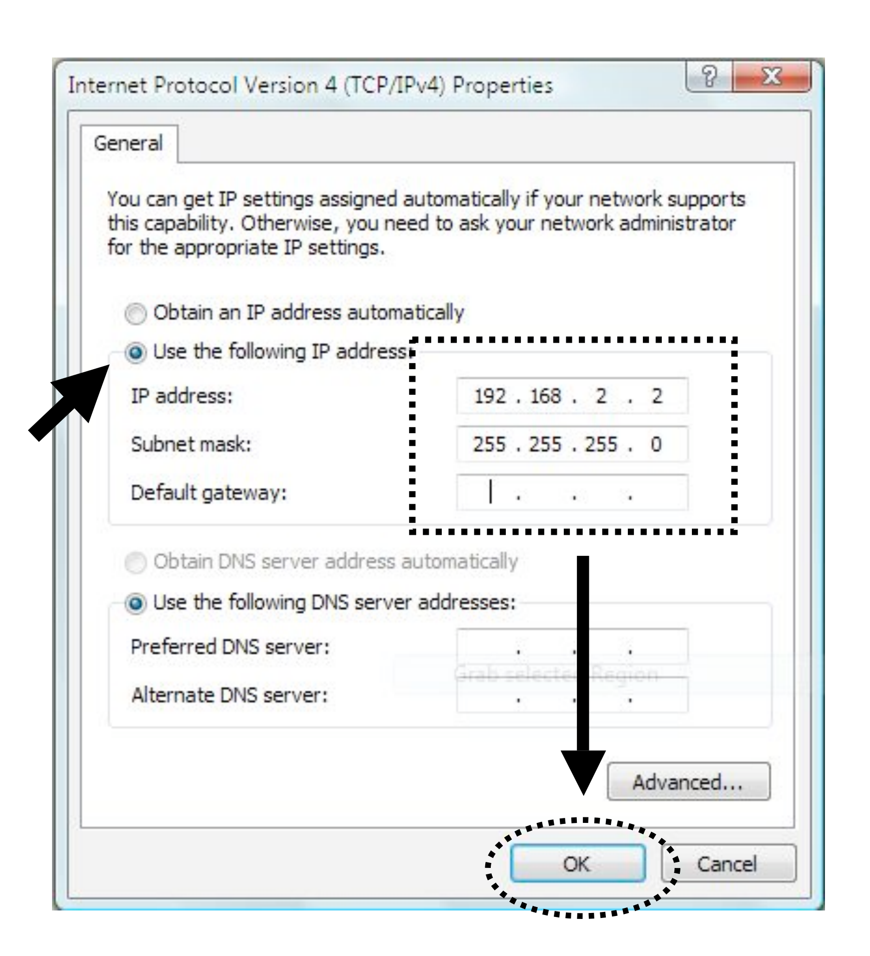
1. Klicken Sie auf Ihrem Desktop unten links auf „Start“, dann auf „Systemsteuerung“. Klicken Sie auf ***Netzwerk- und Freigabecenter***, dann auf ***Netzwerkverbindungen verwalten.*** Rechtsklicken Sie auf ***LAN-Verbindung,*** dann auf “Eigenschaften.” Das ***LAN-Verbindung Eigenschaften*** Fenster öffnet sich. Wählen Sie “Internetprotokoll Version 4 (TCP / IPv4),” dann klicken Sie auf “Eigenschaften.”



2. Wählen Sie “Folgende IP-Adresse verwenden” und geben Sie dann die folgenden Werte in die entsprechenden Felder ein:

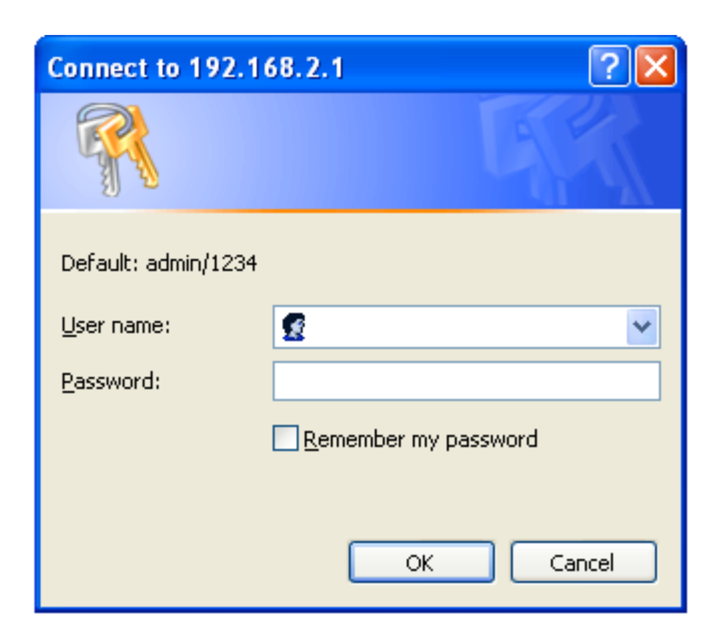
   IP-Adresse: 192.168.2.2
   Subnetzmaske: 255.255.255.0

   Anschließend klicken Sie auf “OK”.

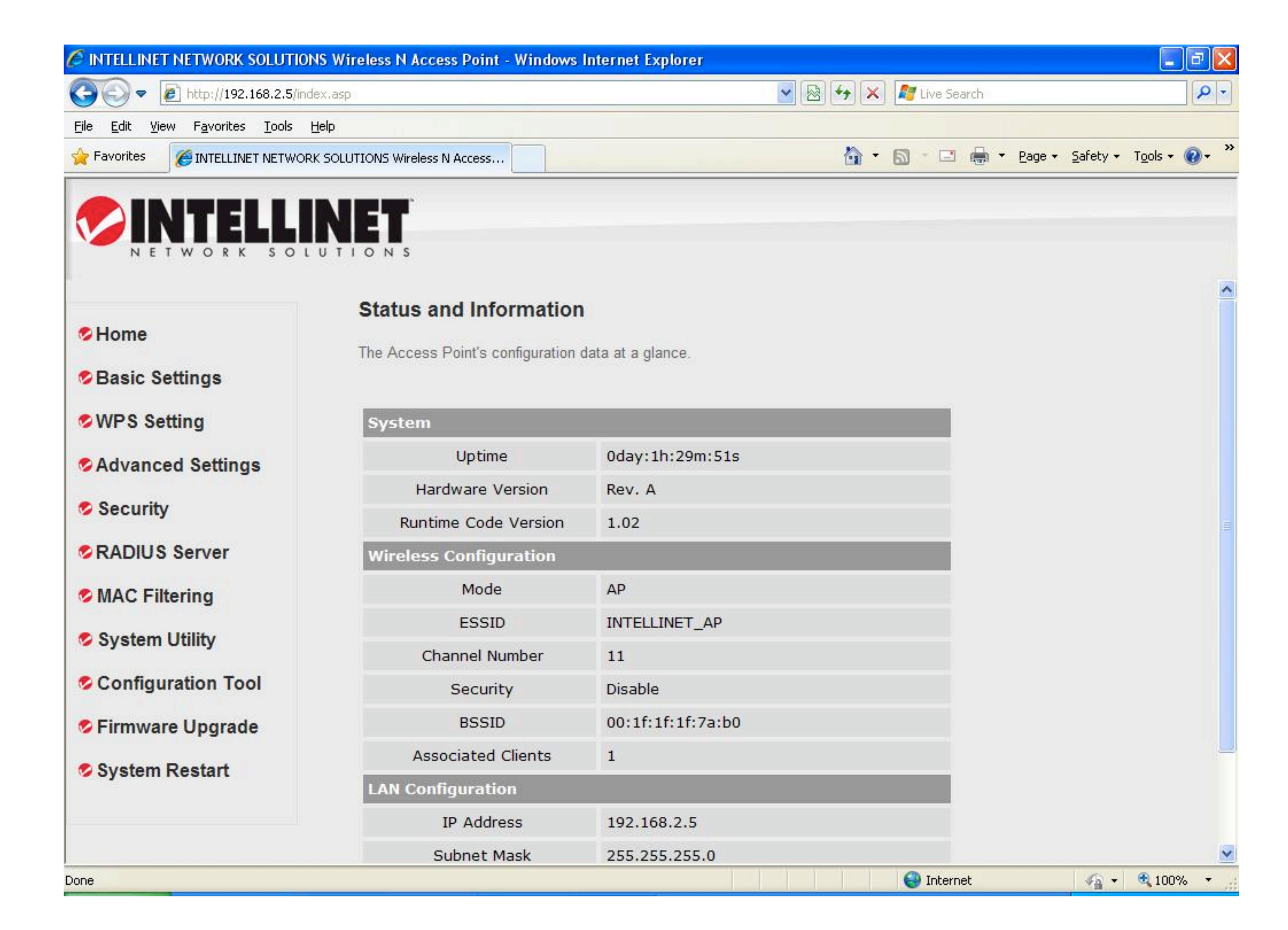

Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 2 . 2
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

2-2-5 Verbindung zur Web-Benutzeroberfläche

Alle Funktionen und Einstellungen dieses Access Points müssen über eine Benutzeroberfläche vorgenommen werden, auf die Sie über den Internetbrowser zugreifen. Öffnen Sie diesen und geben Sie in der Adresszeile “192.168.2.1” ein und drücken Sie Enter. Es öffnet sich folgendes Fenster:



Geben Sie Benutzername und Passwort ein. Der Standard-Benutzername lautet „admin“, und das Standard-Passwort „1234“. Klicken Sie auf „OK”, dann gelangen Sie zur Browser-Benutzeroberfläche dieses Access Points:

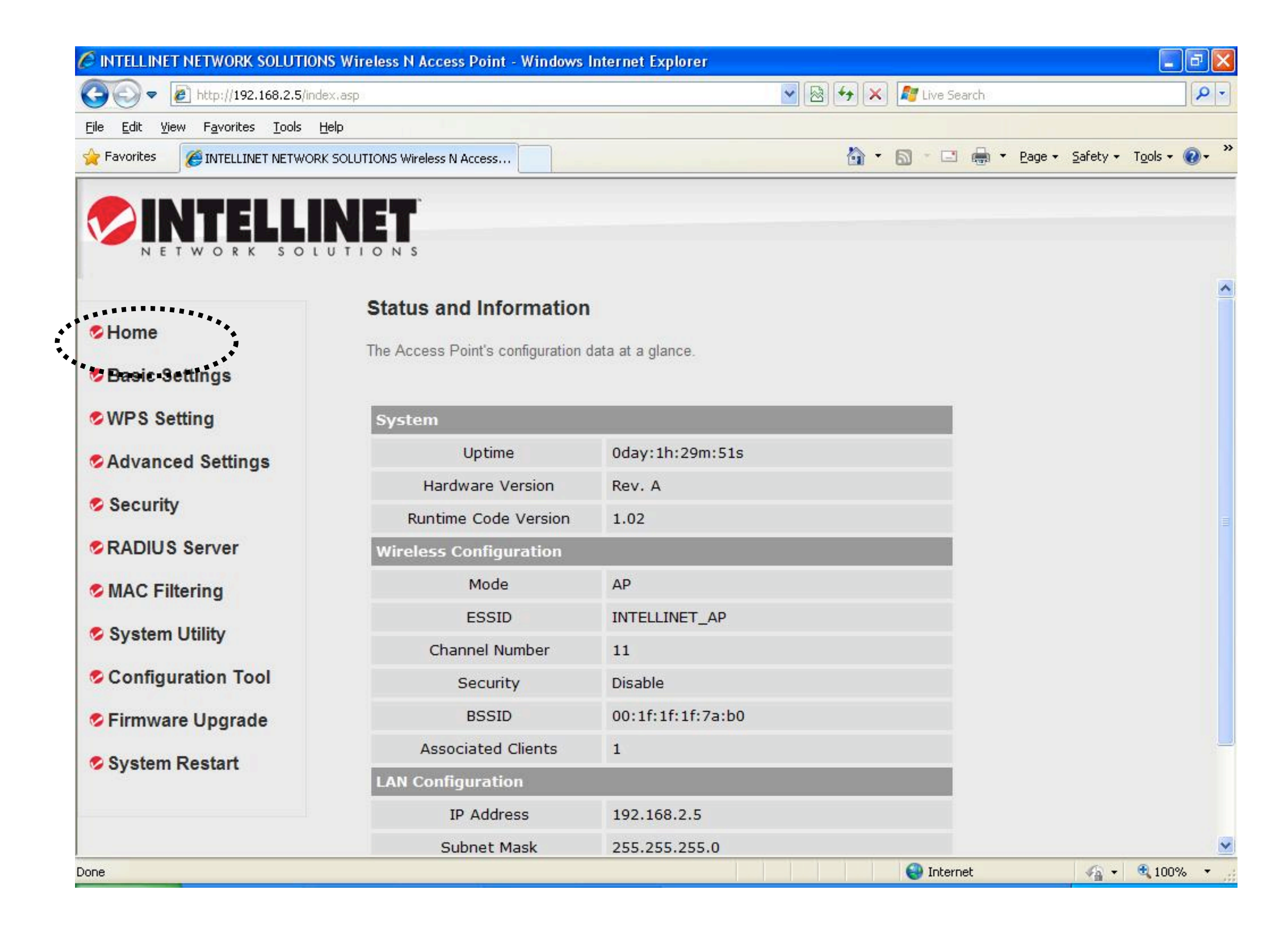


HINWEIS: Wenn Sie diese Benutzeroberfläche in Ihrem Browser nicht sehen können und zur erneuten Eingabe von Benutzername und Passwort aufgefordert werden, haben Sie diese zuvor nicht korrekt eingegeben. Geben Sie die Werte erneut ein. Sind Sie sich absolut sicher, dass Ihre Eingaben korrekt waren, lesen Sie Abschnitt 4: Problemlösungen, um einen Reset durchzuführen und das Standardpasswort wiederherzustellen.

2-3 Systemstatus und -informationen

Nachdem Sie die Verbindung zum Access Point über Ihren Internetbrowser herstellt haben, sehen Sie zunächst die Seite mit Statusinformationen. Hier werden alle Informationen zu System und Netzwerk dieses Access Points dargestellt. Diese Informationen sind hilfreich, wenn Sie technische Details Ihres Access Point erfahren möchten und wenn Sie Verbindungsproblem zwischen Access Point und anderen kabelgebundenen/kabellosen Geräten/Computern beheben möchten.

Sie können in der linken Leiste jederzeit auf „Home" klicken, um zu dieser Informationsseite zurückzukehren. Sie wird folgendermaßen dargestellt:

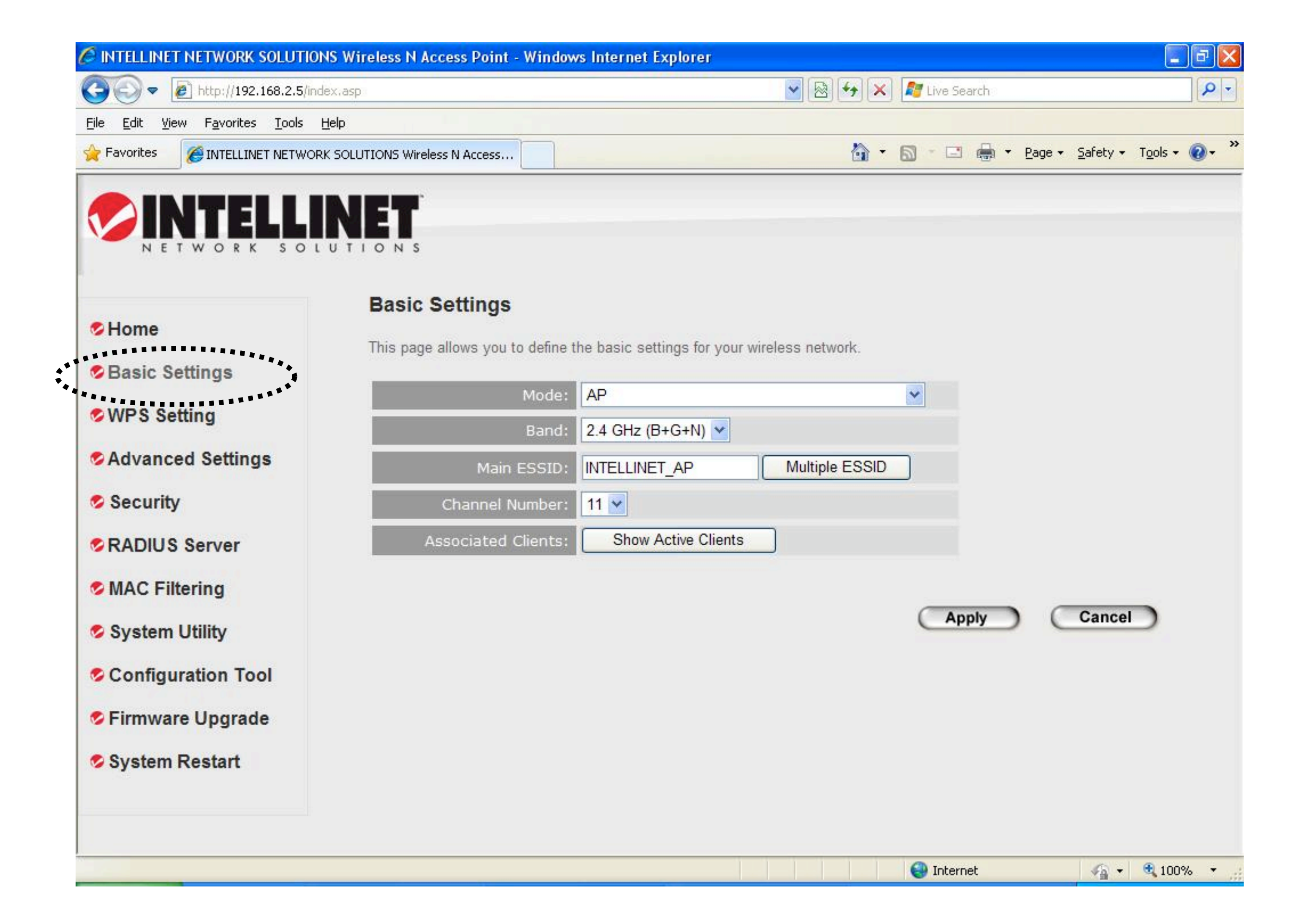


Die Optionen im Einzelnen:

Up time	*Die vergangene Zeit seit der Wireless Access Point das erste Mal eingeschaltet wurde.*
Hardware Version	*Die Hardwareversionsnr. ist nützlich, wenn Sie den Online-Support des Händlers nutzen.*
Runtime Code Version	*Zeigt die aktuelle Firmwareversion. Möchten Sie die Firmware aktualisieren, sehen Sie anhand dieser Nummer, ob eine Aktualisierung notwendig ist.*
Mode	*Zeigt den aktuellen Wireless-Modus (siehe folgender Abschnitt).*
ESSID	*Zeigt die aktuelle ESSID (der Name, der diesen Wireless Access Point identifiziert.*
Channel Number	*Zeigt die aktuelle Wireless Channel-Nummer.*
Security	*Zeigt die aktuellen Wireless Sicherheitseinstellungen.*
BSSID	*Zeigt die aktuelle BSSID (einzigartige ID dieses Access Points, die nicht vom Nutzer geändert werden kann).*
Associated Clients	*Zeigt die Zahl der verbundenen Wireless Clients.*
IP Address	*Zeigt die IP-Adresse diese Wireless Access Points.*
Subnet Mask	*Zeigt die Subnetzmaske der IP-Adresse.*
Default Gateway	*Zeigt die IP-Adresse des Standardgateways.*
MAC address	*Zeigt die MAC-Adresse des LAN-Interfaces.*

2-4 Auswahl eines Betriebsmodus für den Wireless Access Point

Dieser Access Point beherrscht verschiedene Modi: Klicken Sie auf Basic Settings [Grundeinstellungen], um den Betriebsmodus für den jeweils benötigten Zweck auszuwählen.



Klicken Sie auf das Drop-down-Menü „Mode" [Modus], um einen Betriebsmodus auszuwählen. Genauere Beschreibungen jedes Betriebsmodus finden Sie in den folgenden Abschnitten 2-4-1 bis 2-4-6. Es sei vorweggenommen, dass „AP" der gängigste Modus ist, den wir dem Durchschnittnutzer empfehlen.
Es stehen sechs Modi zur Auswahl:

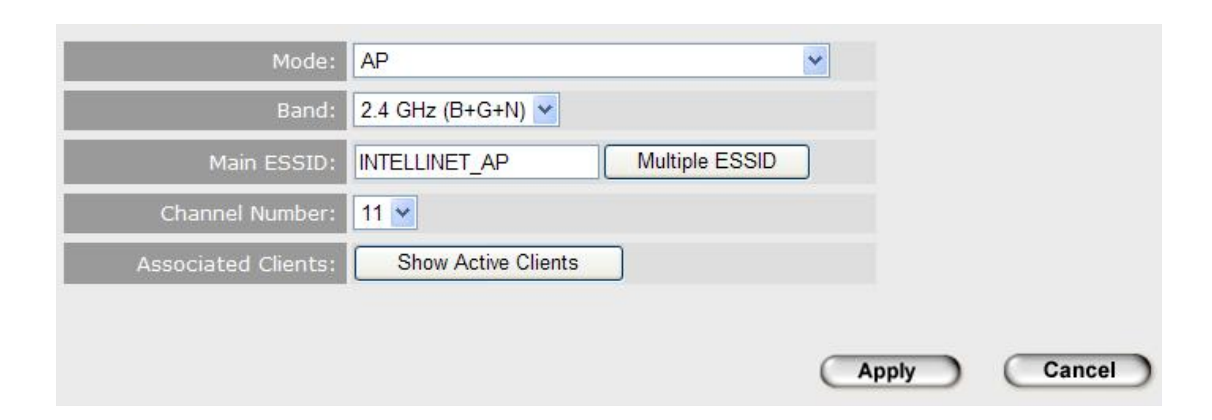
AP	*Ermöglicht Wireless Clients die Verbindung mit dem Access Point und den Datenaus-tausch mit den verbundenen Geräten im kabelgebundenen Netzwerk.*
Station-Infrastructure	*Ermöglicht Ethernet-Geräten wie Fernse-*

	hern und Spielekonsolen die Verbindung als Wireless Client mit dem Access Point.
AP Bridge-Point to Point	*Baut eine Wireless Verbindung zu einem anderen Wireless Access Point auf, der denselben Modus verwendet, vereint die beiden Netzwerke und bezieht auch alle kabelgebundenen Netzwerkgeräte ein. Nur ein weiterer Access Point kann in diesem Modus verbunden werden.*
AP Bridge-Point to Multi-Point	*Baut eine Wireless Verbindung zu anderen Wireless Access Points auf, die denselben Modus verwenden und vereint all diese Netzwerke inklusive der kabelgebundenen Netzwerkgeräte. Bis zu vier weitere Access Points können in diesem Modus verbunden werden.*
AP Bridge-WDS	*Dieser Modus funktioniert ähnlich dem Modus AP Bridge to Multi-Point. Während der Access Point nicht im „Bridge-dedicated“-Modus funktioniert, kann dieser Modus Wireless Clients als Access Point annehmen, während der AP als Wireless Bridge fungiert.*
Universal Repeater	*Dieses Produkt kann als Wireless Repeater (Verstärker) verwendet werden, mit dem Sie die Reichweite Ihres Netzwerks erhöhen können. Der Access Point kann als Station und AP gleichzeitig fungieren. Er kann die Stationsfunktion verwenden, um mit einem Root-AP zu verbinden und die AP-Funktion, um alle Wireless Clients innerhalb seiner Abdeckung zu bedienen.*

2-4-1 AP-Modus

Dies ist der gängigste Modus. Im AP-Modus dient dieser Access Point als Bridge zwischen 802.11b/g/Draft-N Wireless Gerät und einem kabelgebundenen Ethernet-Netzwerk und überträgt Daten zwischen diesen.

Wenn Sie den AP-Modus auswählen, werden folgende Optionen eingeblendet:

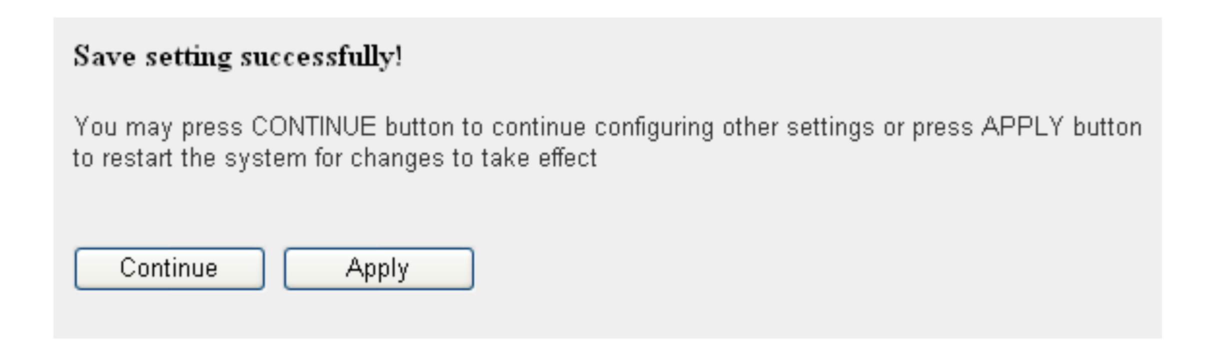


Die Optionen im Einzelnen:

Band	*Wählen Sie die Wireless Bandbreite, die Sie verwenden möchten. Mit verschiedenen Bandbreiteneinstellungen, können Sie Clients mit bestimmter Bandbreite den Zugriff erlauben oder verweigern.* *Je nachdem, welche Bandbreite Sie auswählen (2.4 GHz (B), 2.4 GHz (N) oder 2.4 GHz (G), können sich nur entsprechende Wireless Clients (802.11b, 802.11 Draft-N oder 802.11g) mit diesem Access Point verbinden.* *Mit der Einstellung 2.4 GHz (B+G), können sich nur Wireless Clients mit 802.11b und 802.11g Bandbreiten mit diesem Access Point verbinden.*

	Möchten Sie nur 802.11b, 802.11g und 802.11 Draft-N Clients den Zugriff auf diesen Access Point erlauben, wählen Sie 2.4 GHz (B+G+N) aus.
Main ESSID	*Geben Sie die ESSID (der Name, der diesen Wireless Access Point identifiziert) hier ein. Sie können bis zu 32 alphanumerische Zeichen eingeben.* ***WICHTIG: DIE ESSID UNTERSCHEIDET ZWISCHEN GROSS- UND KLEINSCHREIBUNG.***
Multiple ESSID	*Der Access Point unterstützt mehrere SSID-Funktionen; bis zu vier SSIDs können festgelegt werden. Möchten Sie zusätzliche SSIDs konfigurieren, klicken Sie hier. Für eine genauere Beschreibung dieser Funktion, lesen Sie Abschnitt 2-4-1-1.*
Channel Number	*Wählen Sie die Channel-Nummer, die Sie verwenden möchten. Wenn Sie wissen, dass eine Channel-Nummer von anderen Wireless Access Points in der Umgebung genutzt wird, verwenden Sie eine andere.*
Associated Clients	*Klicken Sie auf „Show Active Clients“ [Aktive Clients anzeigen], worauf sich ein neues Popup-Fenster öffnet, das Informationen über alle Wireless Clients enthält, die mit diesem Access Point verbunden sind. Sie können im Popup-Fenster auf “Refresh” klicken, um die Informationen zu aktualisieren.*

Haben Sie alle Einstellungen vorgenommen, klicken Sie auf „Apply” [Übernehmen], worauf folgende Meldung erscheint:

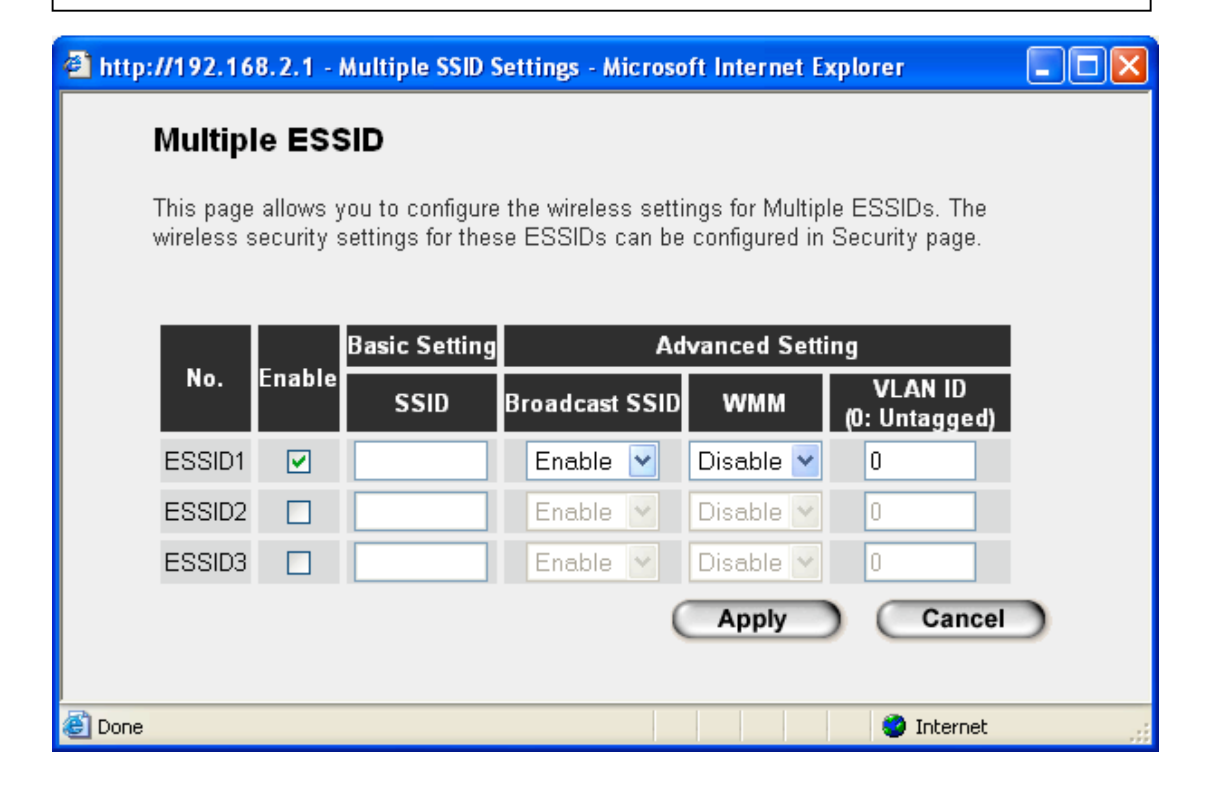


Wird diese Meldung angezeigt, wurden Ihre Einstellungen erfolgreich gespeichert. Klicken Sie auf „Continue” [Fortfahren], um zum vorherigen Einstellungsmenü zurückzukehren oder klicken Sie auf „Apply” [Übernehmen], um den Access Point neu zu starten. Der Neustart dauert ca. 30 Sekunden, danach sind Ihre Änderungen übernommen.

2-4-1-1 Multiple ESSIDs

Dieser Access Point unterstützt vier SSIDs. Mit Ausnahme der Haupt-SSID (diese wird in den Grundeinstellungen konfiguriert), können Sie hier drei weitere SSIDs einstellen. Mit unterschiedlichen SSIDs können Sie separate Wireless Netzwerke mit unterschiedlichen SSID-Namen, Wireless Sicherheits, WMM- und VLAN-Einstellungen festlegen.

HINWEIS: Möchten Sie die Wireless Sicherheitseinstellunge für unterschiedliche SSIDs einstellen, lesen Sie Abschnitt 2-7 Wireless Sicherheit für weitere Informationen.



Die Optionen im Einzelnen:

No.	*Mit Ausnahme der Haupt-SSID, können Sie hier drei drei weitere ESSIDs konfigurieren.*
Enable	*Setzen Sie ein Häkchen um die zusätzlichen ESSIDs zu aktivieren.*
SSID	*Geben Sie den SSID-Namen (den Namen, der diesen Wireless Access Point identifiziert) hier ein. Sie können bis zu 32 alphanumerische*

	Zeichen eingeben. ***WICHTIG: DIE ESSID UNTERSCHEIDET ZWISCHEN GROSS- UND KLEINSCHREIBUNG.***
Broadcast SSID	*Legen Sie fest, ob der Wireless Access Point seine eigene ESSID sendet oder nicht. Sie können die ESSID Ihres Wireless APs verbergen (stellen Sie "Disable" [Deaktivieren] ein), damit sich nur die Nutzer mit Ihrem Wireless AP verbinden können, die Ihre ESSID kennen.*
WMM	*WMM- (Wi-Fi Multimedia) Technologie kann die Performance mancher Netzwerkanwendungen erhöhen. Dazu gehören Audio/ Video-Streaming, VoIP-Telefonie und vieles mehr. Wenn Sie die WMM-Funktion aktivieren, definiert der Access Point die Priorität verschiedener Datenarten. Bei höherer Priorität werden diese Daten sofort verarbeitet. So können Sie ihre Performance erhöhen.*
VLAN ID (0:Untagged)	*Nutzt Ihr Netzwerk VLANs, können Sie diesen eine SSID zuweisen. Client-Geräte, die eine gemeinsame SSID verwenden, können in einem VLAN gruppiert werden. Der VLAN ID-Bereich geht von 1 bis 4094. Die VLAN ID lautet standardmäßig 0, d. h. die VLAN-Funktion für diese ESSID ist deaktiviert.*

2-4-2 Station-Infrastructure

In diesem Modus können Sie den Access Point mit einem Ethernet-Gerät wie Fernseher oder Spielekonsole verbinden, womit Sie das Ethernet-Gerät zu einer Wireless Station machen und so Zugang zu einem Wireless Netzwerk über den Access point oder einen AP Router erhalten.

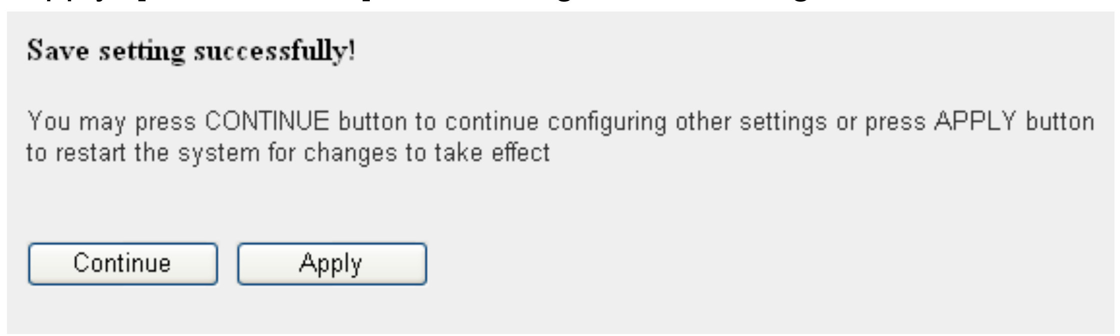
Mode:	Station-Infrastructure
Band:	2.4 GHz (B+G+N)
Main ESSID:	INTELLINET_AP
Site Survey:	Start

Die Optionen im Einzelnen:

Band	*Wählen Sie die Wireless Bandbreite, die Sie verwenden möchten. Mit verschiedenen Bandbreiteneinstellungen, können Sie Clients mit bestimmter Bandbreite den Zugriff erlauben oder verweigern.* *Je nachdem, welche Bandbreite Sie auswählen (2.4 GHz (B), 2.4 GHz (N) oder 2.4 GHz (G), können sich nur entsprechende Wireless Clients (802.11b, 802.11 Draft-N oder 802.11g) mit diesem Access Point verbinden.* *Mit der Einstellung 2.4 GHz (B+G), können sich nur Wireless Clients mit 802.11b und 802.11g Bandbreiten mit diesem Access Point verbinden.* *Möchten Sie nur 802.11b, 802.11g und 802.11 Draft-N Clients den Zugriff auf diesen Access Point erlauben, wählen Sie 2.4 GHz (B+G+N) aus.*
Main ESSID	*Geben Sie die ESSID (der Name, der diesen Wireless Access Point identifiziert) hier ein. Sie können bis zu 32 alphanumerische Zeichen eingeben.* ***WICHTIG: DIE ESSID UNTERSCHEIDET ZWISCHEN GROSS- UND KLEINSCHREIBUNG.***
Site Survey	*Wenn Sie diesen Access Point als Wireless Station für ein Ethernet-Netzwerkgerät verwenden, um dieses Wireless-fähig zu machen,*

	müssen Sie es mit einem aktiven Access Point verbinden. Klicken Sie auf “Select Site Survey” [Umgebungsprüfung] worauf sich die „Wireless Site Survey“-Tabelle öffnet. Dort werden alle verfügbaren nahen Access Points aufgelistet. Sie können einen AP in der Liste auswählen und auf das Wireless Netzwerk über diesen Access Point zugreifen. Weitere Information über die „Wireless Site Survey“-Tabelle finden Sie in Abschnitt 2-4-2-1.

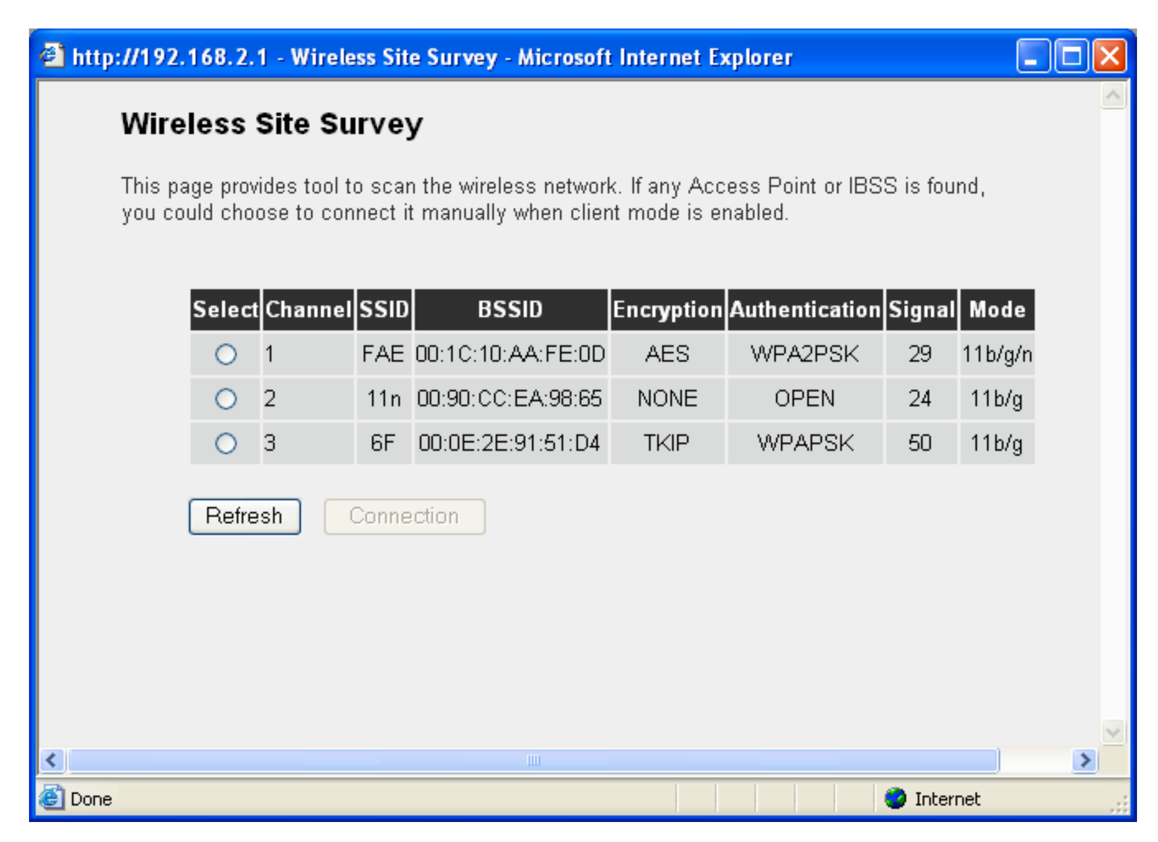
Haben Sie alle Einstellungen vorgenommen, klicken Sie auf „Apply” [Übernehmen], worauf folgende Meldung erscheint:



Wird diese Meldung angezeigt, wurden Ihre Einstellungen erfolgreich gespeichert. Klicken Sie auf „Continue” [Fortfahren], um zum vorherigen Einstellungsmenü zurückzukehren oder klicken Sie auf „Apply” [Übernehmen], um den Access Point neu zu starten. Der Neustart dauert ca. 30 Sekunden, danach wurden Ihre Änderungen übernommen.

2-4-2-1 Wireless Site Survey

Hier werden alle verfügbaren nahen Access Points aufgelistet, da der Access Point im „Station“-Modus aktiv ist. Sie können einen Access Point auswählen, mit dem Sie sich verbinden möchten.



Die Optionen im Einzelnen:

Select	*Wählen Sie hier den Access Point aus.*
Channel	*Zeigt die Channel-Nummer des Access Points.*
SSID	*Zeigt den SSID-Namen des Access Points.*
BSSID	*Zeigt die BSSID (MAC-Adresse) des APs.*
Encryption	*Zeigt die Verschlüsselungseinstellung des Access Points. Wenn Sie einen Access Point mit Sicherheitseinstellungen auswählen, müssen Sie dieselben Sicherheitseinstellungen auf Ihrem AP auswählen. Lesen Sie mehr in Abschnitt 2-7 Wireless Sicherheit.*
Authentication	*Zeigt die Authentifizierungsart dieses Access Points.*
Signal	*Die Signalstärke jedes Access Points wird hier angezeigt. Je stärker das Signal, desto höher die Verbindungsqualität.*
Mode	*Zeigt die Wireless Modi des Access Points: 11b, 11b/g, 11b/g/n oder 11n only.*
Refresh	*Aktualisiert die Liste.*
Connection	*Markieren Sie einen Access Point und klicken*

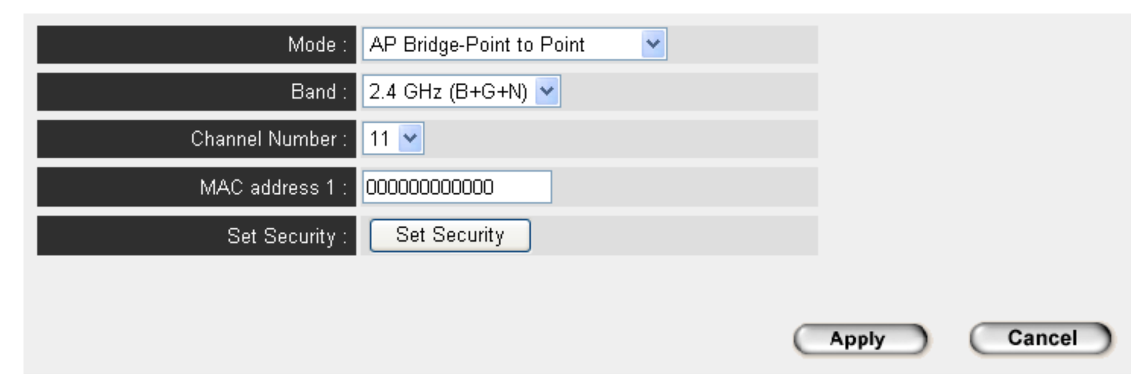
	Sie hier, um das Netzwerk auszuwählen. Der SSID-Name Ihres ausgewählten AP wird in der Haupt-SSID bei den Grundeinstellungen angezeigt.

2-4-3 AP Bridge-Point to Point Modus

In diesem Modus verbindet sich der Wireless Access Point mit einem anderen Wireless AP, der denselben Modus verwendet und allen kabelgebundenen Ethernet-Clients auf beiden Wireless Access Points werden in einem Netzwerk vereint. Sie können diesen Modus nutzen, um sich mit einem anderen Netzwerk zu verbinden, das physisch isoliert ist.

HINWEIS: Wenn Sie Ihren Access Point auf diesen Modus schalten, wird er keine „regulären“ Wireless Clients mehr zulassen.

Wenn Sie AP Bridge-Point to Point auswählen, werden folgende Optionen eingeblendet:

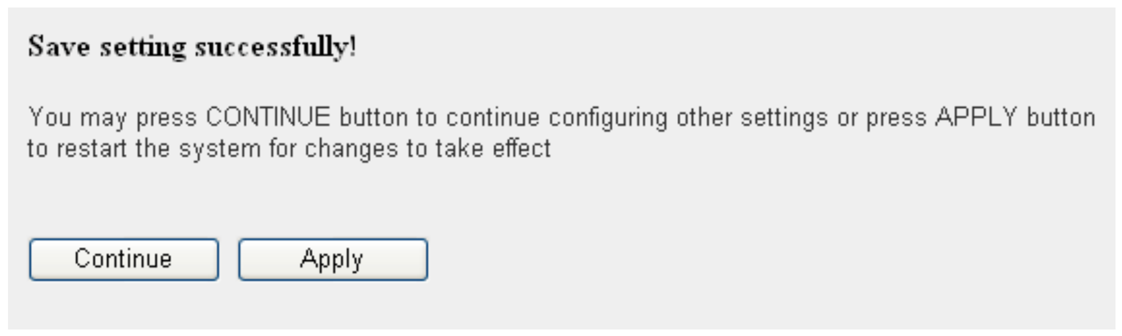


Die Optionen im Einzelnen:

Band	*Wählen Sie die Wireless Bandbreite, die Sie verwenden möchten. Mit verschiedenen Bandbreiteneinstellungen, können Sie Clients mit bestimmter Bandbreite den Zugriff erlauben oder verweigern.* *Je nachdem, welche Bandbreite Sie auswählen (2.4 GHz (B), 2.4 GHz (N) oder 2.4 GHz*

	(G), können sich nur entsprechende Wireless Clients (802.11b, 802.11 Draft-N oder 802.11g) mit diesem Access Point verbinden. *Mit der Einstellung 2.4 GHz (B+G), können sich nur Wireless Clients mit 802.11b und 802.11g Bandbreiten mit diesem Access Point verbinden.* *Möchten Sie nur 802.11b, 802.11g und 802.11 Draft-N Clients den Zugriff auf diesen Access Point erlauben, wählen Sie 2.4 GHz (B+G+N) aus.*
Channel Number	*Wählen Sie die Channel-Nummer aus, die Sie verwenden möchten. Die Channel-Nummer muss mit der des Wireless Access Points identisch sein, mit dem Sie sich verbinden möchten.*
MAC address 1	*Geben Sie die MAC-Adresse des Wireless Access Points ein, mit dem Sie sich verbinden möchten.*
Set Security	*Wählen Sie einen Verschlüsselungsmodus aus. Beim Klick auf diese Schaltfläche öffnet sich ein Popup-Fenster. Weitere Anweisungen finden Sie in Abschnitt 2-7.*

Haben Sie alle Einstellungen vorgenommen, klicken Sie auf „Apply” [Übernehmen], worauf folgende Meldung erscheint:



Wird diese Meldung angezeigt, wurden Ihre Einstellungen erfolgreich gespeichert. Klicken Sie auf „Continue” [Fortfahren], um zum

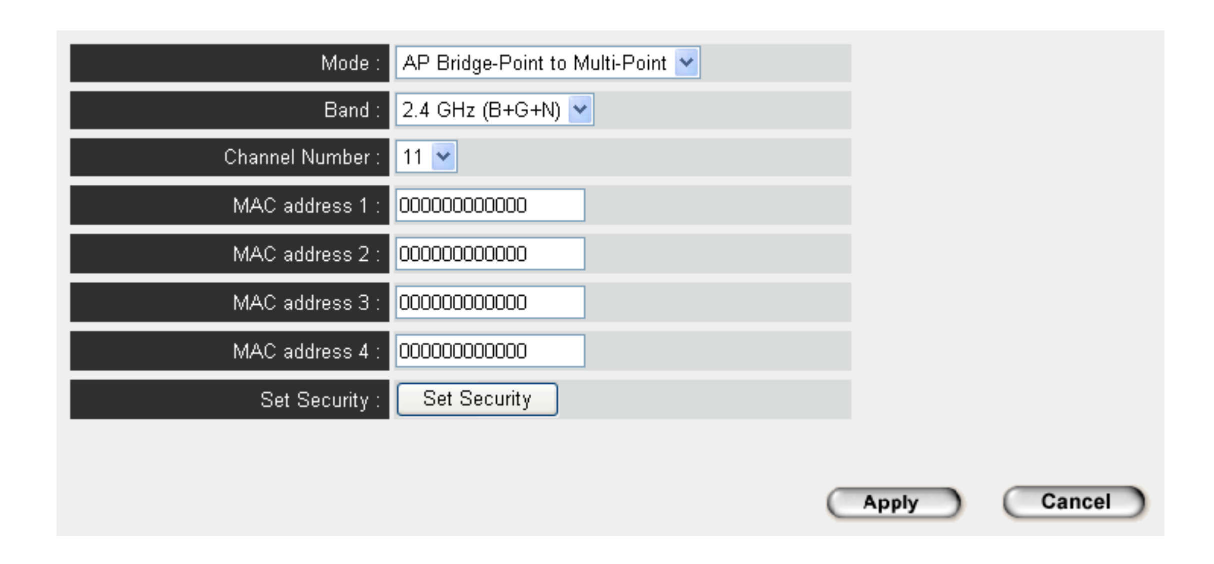
vorherigen Einstellungsmenü zurückzukehren oder klicken Sie auf „Apply” [Übernehmen], um den Access Point neu zu starten. Der Neustart dauert ca. 30 Sekunden, danach wurden Ihre Änderungen übernommen.

2-4-4 AP Bridge-Point to Multi-Point Modus

In diesem Modus verbindet sich der Wireless Access Point mit bis zu vier anderen Wireless AP, die denselben Modus verwenden und allen kabelgebundenen Ethernet-Clients auf beiden Wireless Access Points werden in einem Netzwerk vereint. Sie können diesen Modus nutzen, um ein Netzwerk mit anderen Netzwerken zu verbinden, die physisch isoliert sind.

HINWEIS: Wenn Sie Ihren Access Point auf diesen Modus schalten, wird er keine „regulären“ Wireless Clients mehr zulassen.

Wenn Sie AP Bridge-Point to Multi-Point auswählen, werden folgende Optionen eingeblendet:

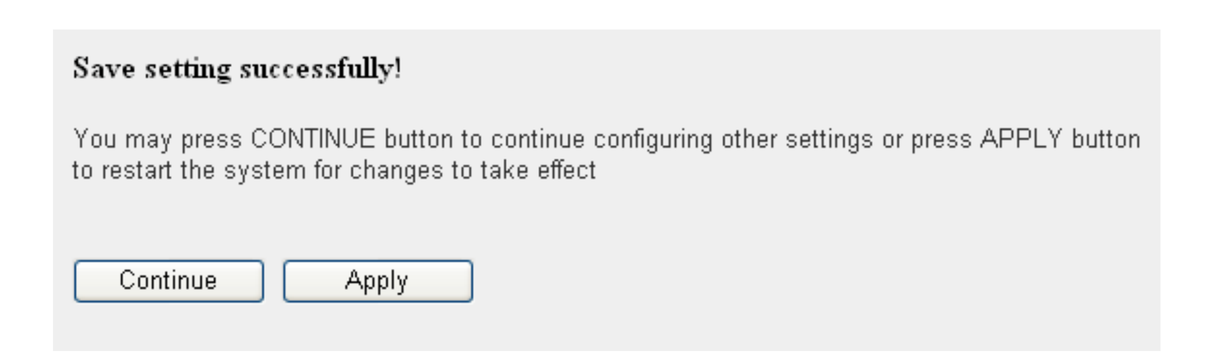


Die Optionen im Einzelnen:

Band	*Wählen Sie die Wireless Bandbreite, die Sie verwenden möchten. Mit verschiedenen Bandbreiteneinstellungen, können Sie Clients mit bestimmter Bandbreite den Zugriff erlauben oder verweigern.* *Je nachdem, welche Bandbreite Sie auswählen (2.4 GHz (B), 2.4 GHz (N) oder 2.4 GHz (G), können sich nur entsprechende Wireless*

	Clients (802.11b, 802.11 Draft-N oder 802.11g) mit diesem Access Point verbinden. *Mit der Einstellung 2.4 GHz (B+G), können sich nur Wireless Clients mit 802.11b und 802.11g Bandbreiten mit diesem Access Point verbinden.* *Möchten Sie nur 802.11b, 802.11g und 802.11 Draft-N Clients den Zugriff auf diesen Access Point erlauben, wählen Sie 2.4 GHz (B+G+N) aus.*
Channel Number	*Wählen Sie die Channel-Nummer aus, die Sie verwenden möchten. Die Channel-Nummer muss mit denen der Wireless Access Points identisch sein, mit denen Sie sich verbinden möchten.*
MAC address 1-4	*Geben Sie die MAC-Adressen der Wireless Access Points ein, mit denen Sie sich verbin-den möchten.*
Set Security	*Wählen Sie einen Verschlüsselungsmodus aus. Beim Klick auf diese Schaltfläche öffnet sich ein Popup-Fenster. Weitere Anweisungen finden Sie in Abschnitt 2-7.*

Haben Sie alle Einstellungen vorgenommen, klicken Sie auf „Ap-ply” [Übernehmen], worauf folgende Meldung erscheint:



Wird diese Meldung angezeigt, wurden Ihre Einstellungen erfolg-reich gespeichert. Klicken Sie auf „Continue” [Fortfahren], um zum

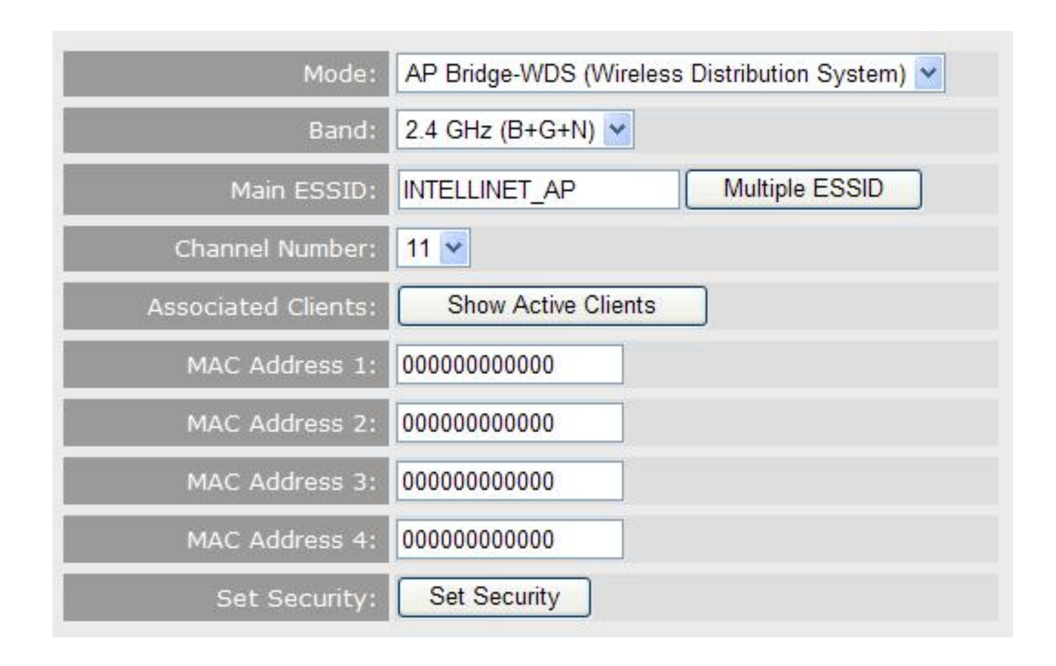
vorherigen Einstellungsmenü zurückzukehren oder klicken Sie auf „Apply" [Übernehmen], um den Access Point neu zu starten. Der Neustart dauert ca. 30 Sekunden, danach wurden Ihre Änderungen übernommen.

2-4-5 AP Bridge-WDS Modus

In diesem Modus verbindet sich der Wireless Access Point mit bis zu vier anderen Wireless AP, die denselben Modus verwenden und allen kabelgebundenen Ethernet-Clients auf beiden Wireless Access Points werden in einem Netzwerk vereint. Sie können diesen Modus nutzen, um ein Netzwerk mit anderen Netzwerken zu verbinden, die physisch isoliert sind.

In diesem Modus lässt der Access Point „reguläre“ Wireless Clients zu.

Wenn Sie AP Bridge-WDS auswählen, werden folgende Optionen eingeblendet:



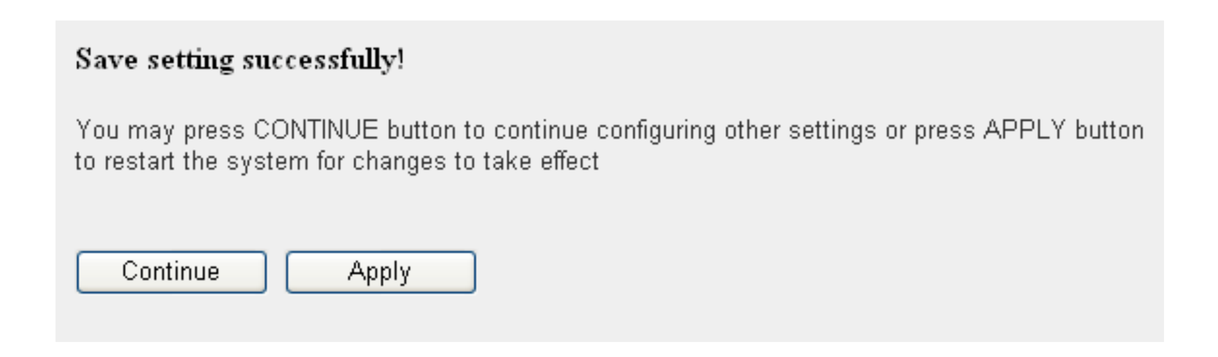
Die Optionen im Einzelnen:

Band	*Wählen Sie die Wireless Bandbreite, die Sie verwenden möchten. Mit verschiedenen Bandbreiteneinstellungen, können Sie Clients mit bestimmter Bandbreite den Zugriff erlauben oder verweigern.* *Je nachdem, welche Bandbreite Sie auswählen (2.4 GHz (B), 2.4 GHz (N) oder 2.4 GHz*

	(G), können sich nur entsprechende Wireless Clients (802.11b, 802.11 Draft-N oder 802.11g) mit diesem Access Point verbinden. *Mit der Einstellung 2.4 GHz (B+G), können sich nur Wireless Clients mit 802.11b und 802.11g Bandbreiten mit diesem Access Point verbinden.* *Möchten Sie nur 802.11b, 802.11g und 802.11 Draft-N Clients den Zugriff auf diesen Access Point erlauben, wählen Sie 2.4 GHz (B+G+N) aus.*
MAIN ESSID	*Geben Sie die ESSID (der Name, der diesen Wireless Access Point identifiziert) hier ein. Sie können bis zu 32 alphanumerische Zeichen eingeben.* ***WICHTIG: DIE ESSID UNTERSCHEIDET ZWISCHEN GROSS- UND KLEINSCHREIBUNG.***
Multiple ESSID	*Der Access Point unterstützt mehrere SSID-Funktionen; bis zu vier SSIDs können festgelegt werden. Möchten Sie zusätzliche SSIDs konfigurieren, klicken Sie hier. Für genauere Anweisungen zu dieser Funktion, lesen Sie Abschnitt 2-4-1-1.*
Channel Number	*Wählen Sie die Channel-Nummer aus, die Sie verwenden möchten. Die Channel-Nummer muss mit der des Wireless Access Points identisch sein, mit dem Sie sich verbinden möchten.*
Associated Clients	*Klicken Sie auf „Show Active Clients“ [Aktive Clients anzeigen], worauf sich ein neues Popup-Fenster öffnet, das Informationen über alle Wireless Clients enthält, die mit diesem Access Point verbunden sind. Sie können im Popup-Fenster auf “Refresh” klicken, um die Informationen zu aktualisieren.*
MAC address 1-4	*Geben Sie die MAC-Adressen der Wireless Access Points ein, mit denen Sie sich verbin-*

	den möchten.
Set Security	*Wählen Sie einen Verschlüsselungsmodus aus. Beim Klick auf diese Schaltfläche öffnet sich ein Popup-Fenster. Lesen Sie Abschnitt 2-7 für genaue Anweisungen.*

Haben Sie alle Einstellungen vorgenommen, klicken Sie auf „Apply” [Übernehmen], worauf folgende Meldung erscheint:



Wird diese Meldung angezeigt, wurden Ihre Einstellungen erfolgreich gespeichert. Klicken Sie auf „Continue” [Fortfahren], um zum vorherigen Einstellungsmenü zurückzukehren oder klicken Sie auf „Apply” [Übernehmen], um den Access Point neu zu starten. Der Neustart dauert ca. 30 Sekunden, danach wurden Ihre Änderungen übernommen.

2-4-6 Universal Repeater

In diesem Modus kann der Access Point als Wireless Repeater- dienen: Er kann Station und AP gleichzeitig sein. Mit der Stationsfunktion kann er sich mit einem Root-AP verbinden und mit der AP-Funktion alle Wireless Stationen innerhalb seiner Reichweite zu bedienen.

HINWEIS: Im Repeater-Modus demoduliert dieser Access Point das empfangene Signal, prüft ob das Signal Interferenzen für den laufenden Netzwerkbetrieb darstellt und dann das Signal noch erneut modulieren und verstärken. Die Ausgangsleistung dieses Modus ist die gleiche wie die des WDS und des normalen AP-Modus.

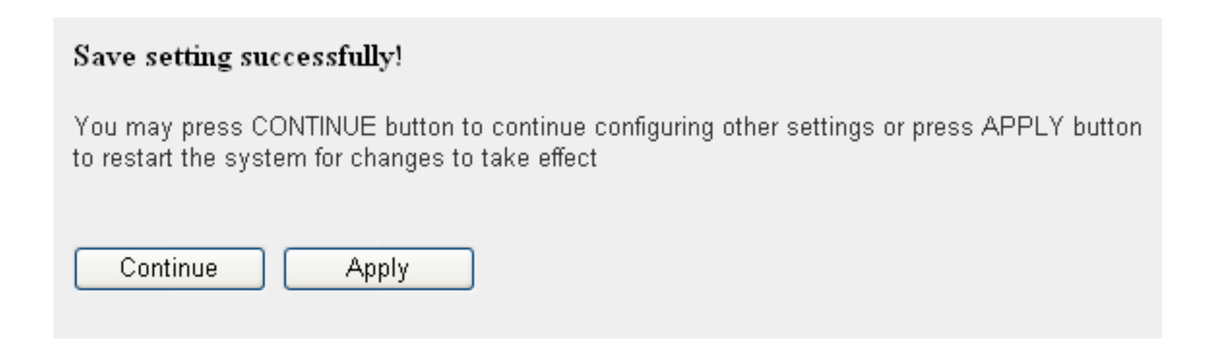
Mode:	Universal Repeater
Band:	2.4 GHz (B+G+N)
Main ESSID:	INTELLINET_AP [Multiple ESSID]
Channel Number:	11
Associated Clients:	[Show Active Clients]
Root AP SSID:	
Wireless Site Survey:	[Wireless Site Survey]

Die Optionen im Einzelnen:

Band	*Wählen Sie die Wireless Bandbreite, die Sie verwenden möchten. Mit verschiedenen Bandbreiteneinstellungen, können Sie Clients mit bestimmter Bandbreite den Zugriff erlauben oder verweigern.* *Je nachdem, welche Bandbreite Sie auswählen (2.4 GHz (B), 2.4 GHz (N) oder 2.4 GHz (G), können sich nur entsprechende Wireless Clients (802.11b, 802.11 Draft-N oder 802.11g) mit diesem Access Point verbinden.* *Mit der Einstellung 2.4 GHz (B+G), können sich nur Wireless Clients mit 802.11b und 802.11g Bandbreiten mit diesem Access Point verbinden.* *Möchten Sie nur 802.11b, 802.11g und 802.11 Draft-N Clients den Zugriff auf diesen Access Point erlauben, wählen Sie 2.4 GHz (B+G+N) aus.*
MAIN SSID	*Geben Sie die ESSID (der Name, der diesen Wireless Access Point identifiziert) hier ein. Sie können bis zu 32 alphanumerische Zeichen eingeben.* ***WICHTIG: DIE ESSID UNTERSCHEIDET ZWISCHEN GROSS- UND KLEINSCHREIBUNG.***

Multiple ESSID	*Der Access Point unterstützt mehrere SSID-Funktionen; bis zu vier SSIDs können festgelegt werden. Möchten Sie zusätzliche SSIDs konfigurieren, klicken Sie hier. Für genauere Anweisungen zu dieser Funktion, lesen Sie Abschnitt 2-4-1-1.*
Channel Number	*Wählen Sie die Channel-Nummer aus, die Sie verwenden möchten. Die Channel-Nummer muss mit der des Wireless Access Points identisch sein, mit dem Sie sich verbinden möchten.*
Associated Clients	*Klicken Sie auf „Show Active Clients“ [Aktive Clients anzeigen], worauf sich ein neues Popup-Fenster öffnet, das Informationen über alle Wireless Clients enthält, die mit diesem Access Point verbunden sind. Sie können im Popup-Fenster auf “Refresh” klicken, um die Informationen zu aktualisieren.*
Root AP SSID	*Im Universal-Repeater-Modus, kann dieses Gerät als Station dienen, um eine Verbindung mit einem Root-AP herzustellen. Sie sollten die SSID Root-APs hier zuweisen oder auf „Select Site Survey” [Umgebungsprüfung] klicken, um einen Root-AP auszuwählen.*
Select Site Survey	*Klicken Sie auf “Select Site Survey”, woraufhin sich eine „Wireless Site Survey“ Tabell“ öffnet. Diese listet alle verfügbaren Access Points in der Nähe auf. Sie können einen AP in der Liste auswählen und dieser wird daraufhin zu Ihrem Wireless LAN hinzugefügt. In Abschnitt 2-4-2-1 finden weitere Informationen über die Wireless Site Survey Tabelle.*

Haben Sie alle Einstellungen vorgenommen, klicken Sie auf „Apply” [Übernehmen], worauf folgende Meldung erscheint:



Wird diese Meldung angezeigt, wurden Ihre Einstellungen erfolgreich gespeichert. Klicken Sie auf „Continue” [Fortfahren], um zum vorherigen Einstellungsmenü zurückzukehren oder klicken Sie auf „Apply” [Übernehmen], um den Access Point neu zu starten. Der Neustart dauert ca. 30 Sekunden, danach wurden Ihre Änderungen übernommen.

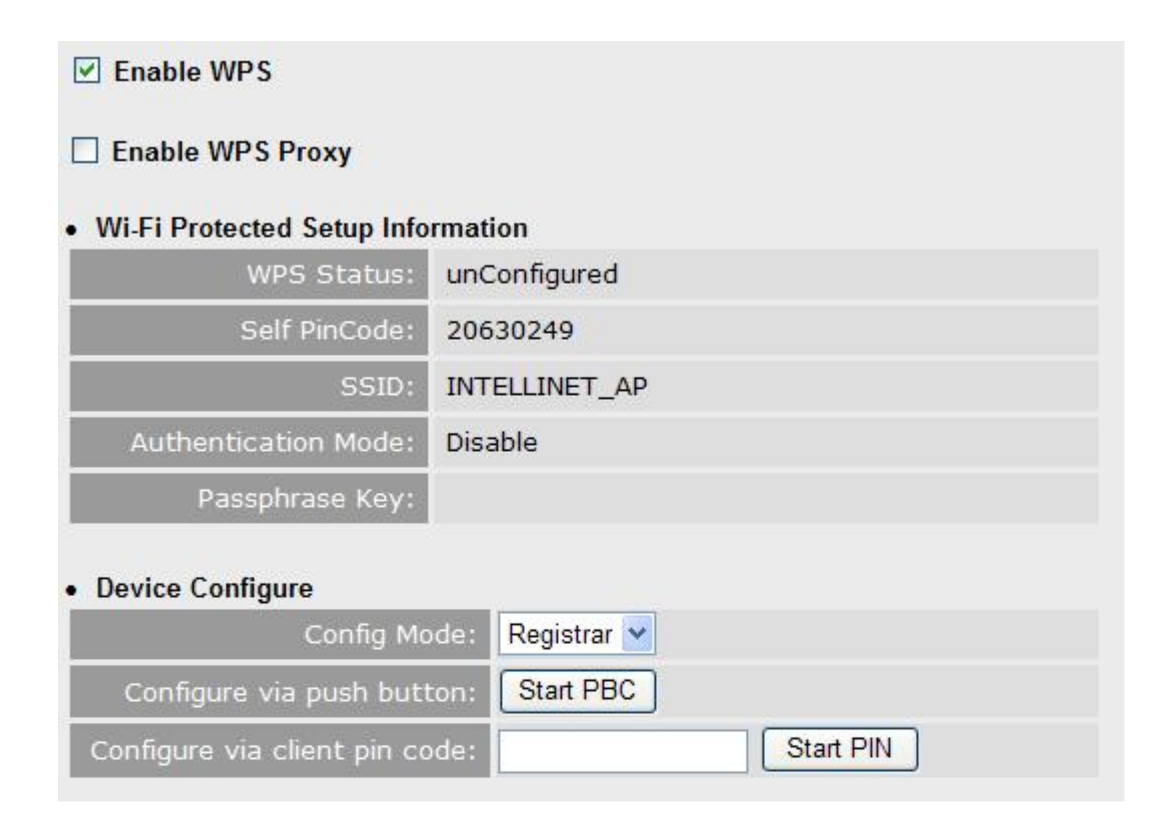
2-5 WPS-Einstellungen

Wi-Fi Protected Setup (WPS) ist der einfachste Weg, um eine Verbindung zwischen Wireless Netzwerk-Clients und diesem Access Point herzustellen. Sie müssen nicht jedes Mal, wenn Sie einen Wireless Client einrichten einen Verschlüsselungsmodus auswählen und eine lange Zeichenfolge eingeben: Sie müssen nur beim Wireless Client und an diesem Access Point einen Knopf betätigen und das WPS übernimmt die Einrichtung für Sie.

Dieser Access Point unterstützt zwei WPS-Arten: Push-Button Configuration (PBC) [Konfiguration auf Knopfdruck] und PIN Code. Möchten Sie PBC verwenden, schalten Sie diesen Access Point in den WPS-Modus und drücken Sie einen speziellen Knopf beim Wireless Client, um den WPS-Modus zu starten. Dazu können Sie entweder den Reset/WPS-Knopf dieses Access Points drücken oder auf „Start PBC" auf der Web-Benutzeroberfläche klicken. Möchten Sie den PIN-Code-Modus verwenden, müssen Sie dem Access Point den PIN Code des Wireless Clients zur Verfügung stellen und den Client anschließend in den WPS-Modus schalten. Danach schalten Sie den Wireless Client in den WPS-Modus. Genaue Anweisungen finden Sie im Folgenden.

HINWEIS: Die WPS-Funktion dieses Access Points funktioniert nicht mit Wireless Clients, die kein WPS unterstützen.

Um mit der WPS-Funktion eine verschlüsselte Verbindung zwischen diesem Access Point und einen WPS-fähigen Wireless Client, klicken Sie links in der Web-Benutzeroberfläche auf „WPS Setting" [WPS-Einstellungen], worauf folgende Informationen eingeblendet werden:



Die Optionen im Einzelnen:

Enable WPS	*Aktiviert oder deaktiviert die WPS-Funktion.*
Wi-Fi Protected Setup Information	*Alle Informationen zu WPS werden hier dargestellt — dies ist nützlich, wenn Sie Verbindungen über WPS herstellen möchten.* *WPS Status: Zeigt den WPS-Status. Wenn die Datenverschlüsselungseinstellungen dieses Access Points noch nicht vorgenommen wurden, steht dort die Statusmeldung "unConfigured" (siehe Abschnitt 2-7 für weitere Informationen). Wurden die Verschlüsselungsein stellungen bereits vorgenommen, steht hier die Meldung „Configured".* *Self PinCode: Dies ist der WPS PIN Code dieses Access Points. Dieser Code ist nützlich, wenn Sie Wireless Verbindungen über WPS mit anderen WPS-fähigen Wireless Geräten herstellen möchten.*

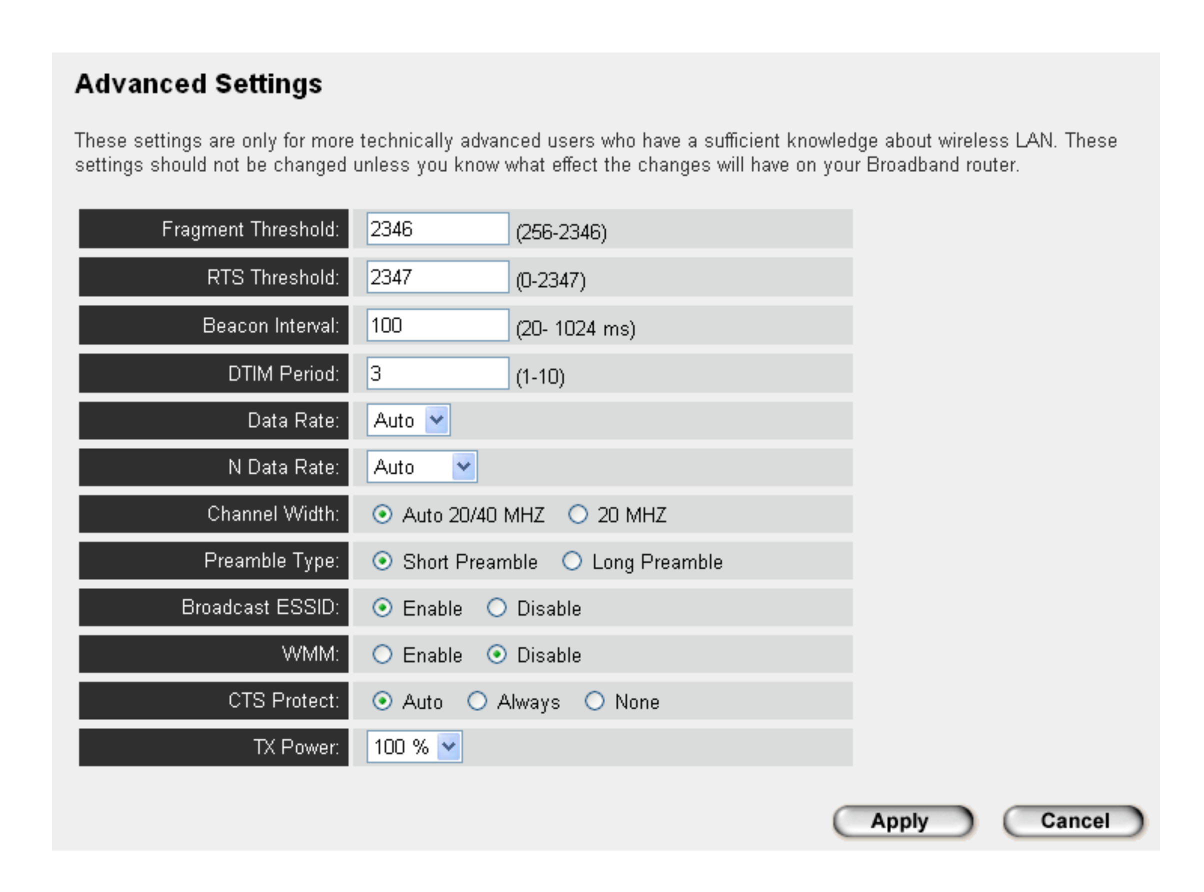
	SSID: Zeigt die SSID (ESSID) dieses APs. Authentifizierungsmodus: Der Wireless Sicherheit Authentifizierungsmodus dieses Access Points wird hier gezeigt. Aktivieren Sie hier die Sicherheitsfunktion dieses Access Point bevor WPS aktiviert ist, wird der AP automatisch den Sicherheitsmodus auf WPA stellen (AES) und eine Reihe von Zeichenfolgenschlüsseln für die WPS-Verbindung erstellen. *Passphrase Key: Zeigt die WPA Zeichenfolge. Alle Zeichen werden aus Sicherheitsgründen als Sternchen dargestellt. Wenn die Verschlüsselung auf diesem Access Point, noch nicht eingestellt wurde, bleibt dieses Feld leer.*
Config Mode	*Es sind die Modi “Registrar” und “Enrollee” [Antragssteller] für die WPS-Verbindung verfügbar. Wenn “Registrar” aktiviert ist, reagieren die Wireless Clients entsprechend der Wireless Einstellungen für WPS-Verbindungen. Wenn der „Enrollee”-Modus aktiviert ist, verhält sich der AP bei der WPS-Verbindung entsprechend der Wireless Einstellungen der Wireless Clients.*
Start PBC	*Ein Klick startet den Push Button-style WPS Installationsvorgang. Dieser Access Point wartet 2 Minuten auf WPS-Anfragen von Wireless Clients. Die WLAN-LED-Anzeige am Access Point leuchtet 2 Minuten lang, wenn dieser auf ankommende WPS-Anfragen wartet.*
Start PIN	*Geben Sie den PIN Code des Wireless Clients ein, mit dem Sie sich verbinden möchten und klicken Sie auf „Start PIN.” Die WLAN-LED-Anzeige am Access Point leuchtet, wenn dieser auf ankommende WPS-Anfragen wartet.*

HINWEIS: Wenn Sie die PBC-Konfiguration als WPS-Einstellung auswählen, müssen Sie die „PBC"-Schaltfläche (an der Hardware oder in der Software) am Wireless Client innerhalb von 120 Sekunden betätigen; tun Sie dies nicht innerhalb dieser Zeitspanne, betätigen Sie die „PBC"-Schaltfläche (Hardware oder Software) erneut.

2-6 Advanced Wireless Settings [Erweiterte Wireless Einstellungen]

Dieser Wireless Access Point verfügt über zahlreiche erweiterte Wireless Eigenschaften. Alle hier aufgelistete Einstellungen richten sich an fortgeschrittene Nutzer: Sind Sie sich bei Bedeutung und Funktion dieser Einstellungen unsicher, ändern Sie sie nicht, ansonsten wird die Wireless Performance evtl. beeinträchtigt.

Klicken Sie auf Advanced Settings, woraufhin folgende Meldung angezeigt wird:



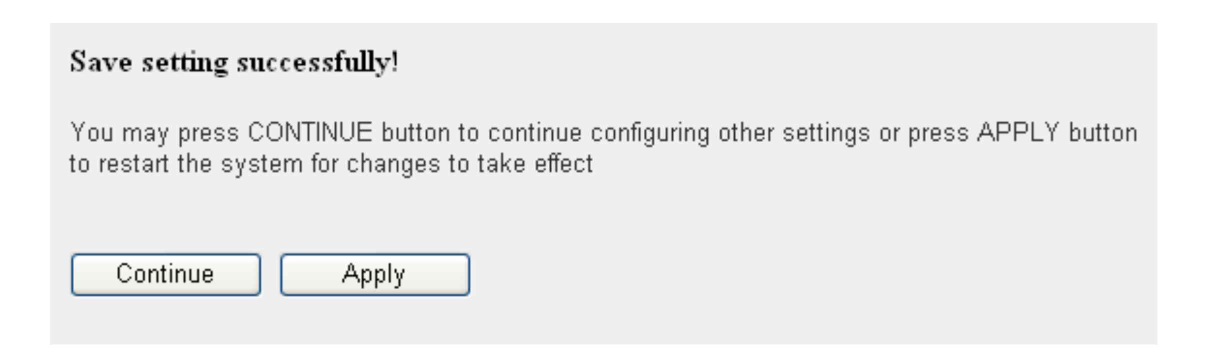
Die Optionen im Einzelnen:

Fragment Threshold	*Legen Sie den Fragment Threshold [Fragmentgrößengrenze] fest.* ***Ändern Sie den Standardwert (2346) nicht, wenn Sie die Auswirkungen nicht kennen.***
RTS Threshold	*Legen Sie den Schwellenwert des RTS (Ready To Send)-Signals fest.* ***Ändern Sie den Standardwert (2347) nicht, wenn Sie die***

	Auswirkungen nicht kennen.
Beacon Interval	*Legen Sie den Abstand der Beacon-Intervalle fest.* ***Ändern Sie den Standardwert (100) nicht, wenn Sie die Auswirkungen nicht kennen.***
DTIM Period	*Legen Sie den Abstand der DTIM-Intervalle fest.****Ändern Sie den Standardwert (3) nicht, wenn Sie die Auswirkungen nicht kennen.***
Data Rate	*Setzen Sie die Wireless Datenübertragungsrate auf einen bestimmten Wert. Da sich die meisten Wireless Geräte automatisch abstimmen und angemessene Datenübertragungsrate festlegen,* ***ist es nicht notwendig diesen Wert zu ändern, es sei denn, Sie kennen die entsprechenden Auswirkungen ganz genau.***
N Data Rate	*Legen Sie die Datenrate von 802.11 Draft-N Clients fest: MCS 0 bis MCS 15: Sie können diesen Wert problemlos auf „Auto“ setzen und es ist* ***nicht notwendig diesen Wert zu ändern, es sei denn, Sie kennen die entsprechenden Auswirkungen ganz genau.***
Channel Width	*Stellen Sie die Wireless Channelbreite (Signalbandbreite dieses Access Points). Wir empfehlen den Wert „Auto 20/40 MHz.” Ändern Sie ihn nicht auf „20 MHz“, es sei denn, Sie kennen die entsprechenden Auswirkungen.*
Preamble Type	*Legen Sie die Art der Präambel fest.* ***Ändern Sie den Standardwert („Short Preamble“) nicht, wenn Sie die Auswirkungen nicht kennen.***
Broadcast ESSID	*Entscheiden Sie, ob der Access Point seine eigene ESSID (Extended Service Set Identity) senden soll oder nicht. Sie können die ESSID Ihres APs verbergen (stellen Sie „Disable“ ein), damit sich nur die Nutzer mit Ihrem Access Point verbinden können, die die ES-*

	SID kennen.
WMM	*WMM- (Wi-Fi Multimedia) Technologie kann die Performance mancher Netzwerkanwendungen erhöhen. Dazu gehören Audio/Video-Streaming, VoIP-Telefonie und vieles mehr. Wenn Sie die WMM-Funktion aktivieren, definiert der Access Point die Priorität verschiedener Datenarten. Bei höherer Priorität werden diese Daten sofort verarbeitet. So können Sie ihre Performance erhöhen.*
CTS Protect	*Die Aktivierung dieser Einstellung verringert das Risiko von Signalinterferenzenen zwischen 802.11b und 802.11g Wireless Access Points. Es wird empfohlen, diese Einstellung auf „Auto“ zu belassen.*
TX Power	*Legt die Ausgangsleistung der Wireless Signale fest. So lange Sie den AP nicht in sehr weiten Umgebungen verwenden, müssen Sie diesen Wert nicht auf 100% setzen.* ***Dies erhöht die Sicherheit (unbefugte Nutzer außerhalb der definierten Reichweite werden nicht in der Lage sein, auf den AP zuzugreifen).***

Haben Sie alle Einstellungen vorgenommen, klicken Sie auf „Apply” [Übernehmen], worauf folgende Meldung erscheint:



Wird diese Meldung angezeigt, wurden Ihre Einstellungen erfolgreich gespeichert. Klicken Sie auf „Continue” [Fortfahren], um zum vorherigen Einstellungsmenü zurückzukehren oder klicken Sie auf

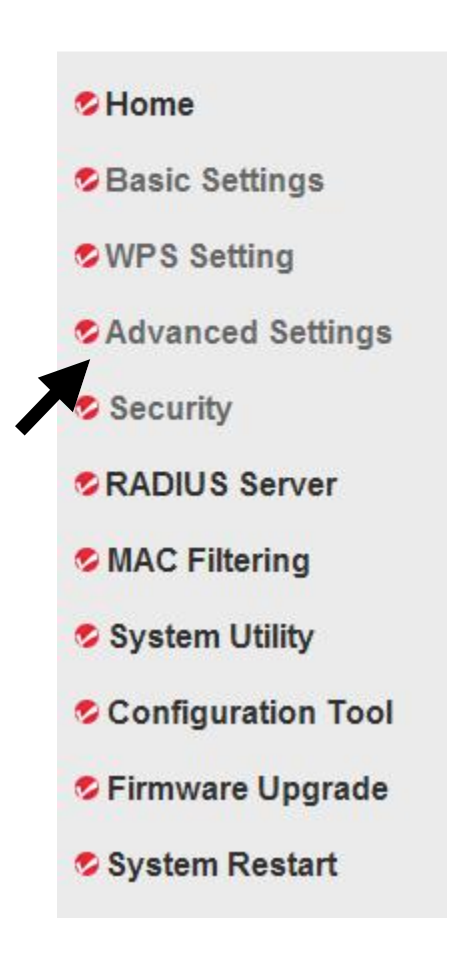
„Apply” [Übernehmen], um den Access Point neu zu starten. Der Neustart dauert ca. 30 Sekunden, danach wurden Ihre Änderungen übernommen.

2-7 Wireless Security [Wireless Sicherheit]

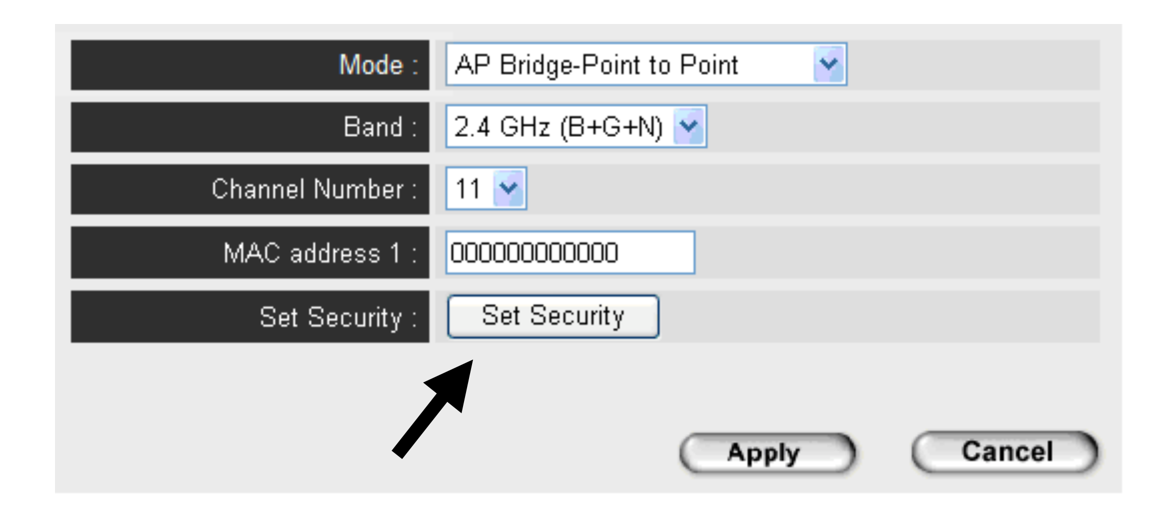
Dieser Wireless Access Point bietet zahlreiche Arten von Wireless Sicherheit (Wireless Datenverschlüsselung). Wenn Sie Datenverschlüsselung verwenden, werden die übertragenen Signale für die Nutzer unleserlich, die den korrekten Schlüssel (Passwort) nicht kennen.

Es gibt zwei Möglichkeiten, die Sicherheitseinstellungen vorzunehmen:

1. Klicken Sie auf „Security“ [Sicherheit] auf der linken Seite der Web-Benutzeroberfläche.



2. Klicken Sie auf “Set Security”, wenn Sie als Betriebsmodus „AP Bridge-Point to Point“, „AP Bridge-Point to Multi-Point“ oder „AP Bridge-WDS“ ausgewählt haben.



Es stehen Ihnen vier Sicherheitsstufen zur Auswahl: Sie können auswählen: „Disable“ (keine Sicherheit – Datenverschlüsselung deaktiviert), WEP, WPA Pre-shared Key und WPA RADIUS. Genauere Anweisungen lesen Sie in den folgenden Abschnitten.

HINWEIS: Haben Sie die Multiple SSID-Funktion aktiviert, wählen Sie zuvor das SSID-Netzwerk, das Sie konfigurieren möchten.

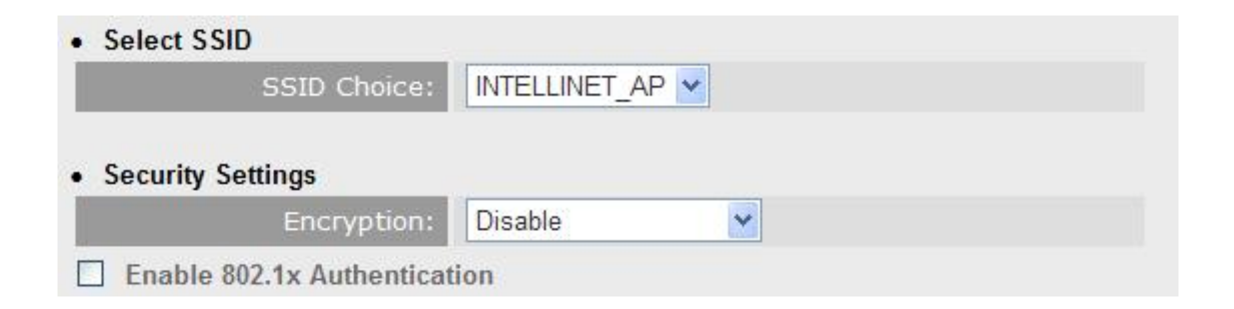
Seien Sie sich der Wichtigkeit von korrekten Sicherheitseinstellungen bewusst! Ohne diese können Hacker auf Ihr lokales Netzwerk zugreifen und auf Ihren Computern und Servern massiven Schaden anrichten.

Sie haben mehrere Möglichkeiten Ihre Wireless Sicherheit zu erhöhen:

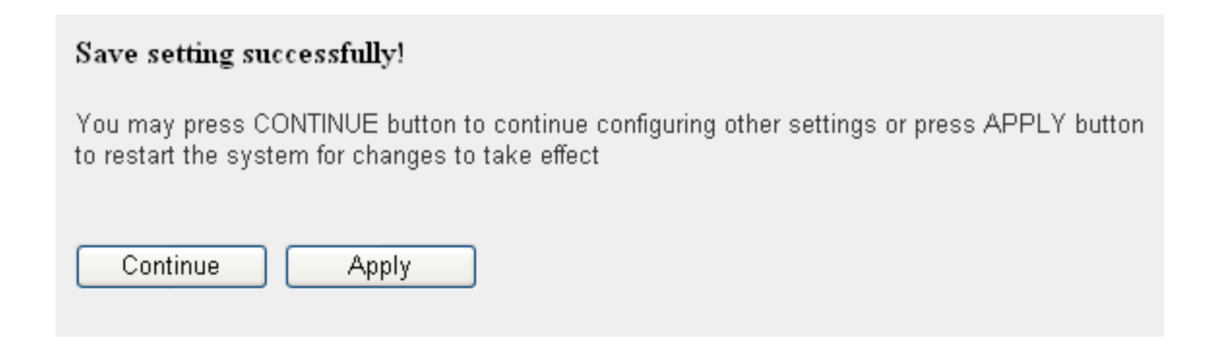
1. Halten Sie die Datenverschlüsselung immer aktiviert. Deaktivieren Sie sie nur, wenn Sie Ihren Access Point öffentlich zugänglich machen möchten.
2. Verwenden Sie niemals einfache Verschlüsselungspasswörter. Verwenden Sie vorzugsweise zufällige Kombinationen von Zahlen und Buchstaben, was die Sicherheit drastisch erhöht.
3. Verwenden Sie möglichst WPA — dieser Standard ist sicherer als WEP.
4. Ändern Sie Ihr Verschlüsselungspasswort regelmäßig.

2-7-1 Disable Security [Sicherheit deaktivieren]

Wählen Sie die SSID aus, die Sie konfigurieren möchten. Wenn Sie "Disable," auswählen, wird die Wireless Verschlüsselung für Ihr Netzwerk deaktiviert.



Haben Sie alle Einstellungen vorgenommen, klicken Sie auf „Apply" [Übernehmen], worauf folgende Meldung erscheint:



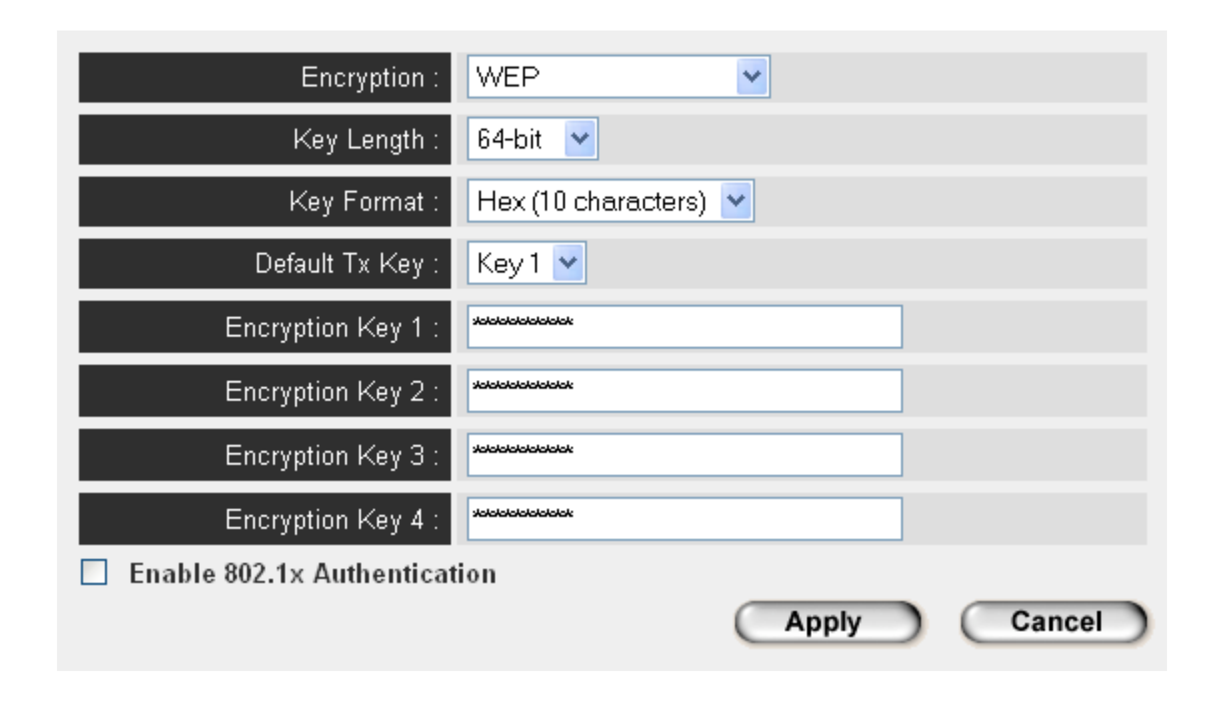
Wird diese Meldung angezeigt, wurden Ihre Einstellungen erfolgreich gespeichert. Klicken Sie auf „Continue" [Fortfahren], um zum vorherigen Einstellungsmenü zurückzukehren oder klicken Sie auf „Apply" [Übernehmen], um den Access Point neu zu starten. Der Neustart dauert ca. 30 Sekunden, danach wurden Ihre Änderungen übernommen.

2-7-2 WEP

WEP (Wired Equivalent Privacy) ist ein gängiger Verschlüsselungsstandard, sicher genug für die Heimnutzung. Sollten Sie einen höheren Sicherheitsstandard benötigen, verwenden Sie WPA-Verschlüsselung (siehe folgender Abschnitt).

Manche Wireless Clients unterstützen kein WPA (nur WEP), daher ist WEP immer noch eine gute Wahl, wenn sich ein solcher Client in Ihrem Netzwerk befindet.

Wenn Sie WEP als Verschlüsselungsart auswählen, öffnet sich folgendes Fenster:

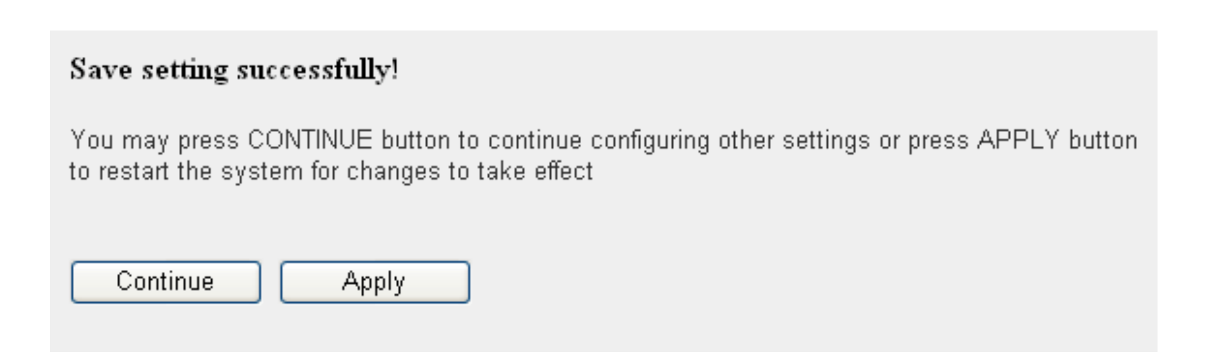


Die Optionen im Einzelnen:

Key Length	*Es gibt zwei WEP-Schlüssellängen: 64-bit und 128-bit. "128-bit" ist sicherer, aber reduziert Ihre Übertragungsperformance.*
Key Format	*Es gibt zwei Schlüsselformate: ASCII und Hex. Wenn Sie ein Format auswählen, wird die Zahl der Zeichen eingeblendet. Wählen Sie beispielsweise "64-bit" als Schlüssellänge und*

	“Hex” als Schlüsselformat, sehen Sie, dass der Schlüssel aus zehn Zeichen besteht.
Default Tx Key	*Sie können bis zu vier WEP-Schlüsselsets definieren und hier entscheiden welcher standardmäßig verwendet werden soll.* ***Wenn Sie sich unsicher sind, wählen Sie „Key 1“ [Schlüssel 1].***
Encryption Key 1 to 4	*Geben Sie hier die Zeichen des WEP-Schlüssels ein. Die Anzahl der Zeichen muss mit der Anzahl im „Key Format“-Feld übereinstimmen. Sie können alle alphanumerischen Zeichen (0-9, a-z, und A-Z) verwenden, wenn Sie „ASCII“-Schlüsselformat auswählen. Wenn Sie „Hex“ als Schlüsselformat auswählen, können Sie nur die Zeichen 0-9, a-f und A-F verwenden. Sie müssen hier mindestens einen WEP-Schlüssel eingeben, geben Sie mehrere ein, sollten diese nicht identisch sein.*
Enable 802.1x Authentication	*Setzen Sie ein Häkchen, um die 802.1x-Benutzerauthentifizierung zu aktivieren. Genauere Anweisungen finden Sie im Abschnitt 2-7-5.*

Haben Sie alle Einstellungen vorgenommen, klicken Sie auf „Apply” [Übernehmen], worauf folgende Meldung erscheint:

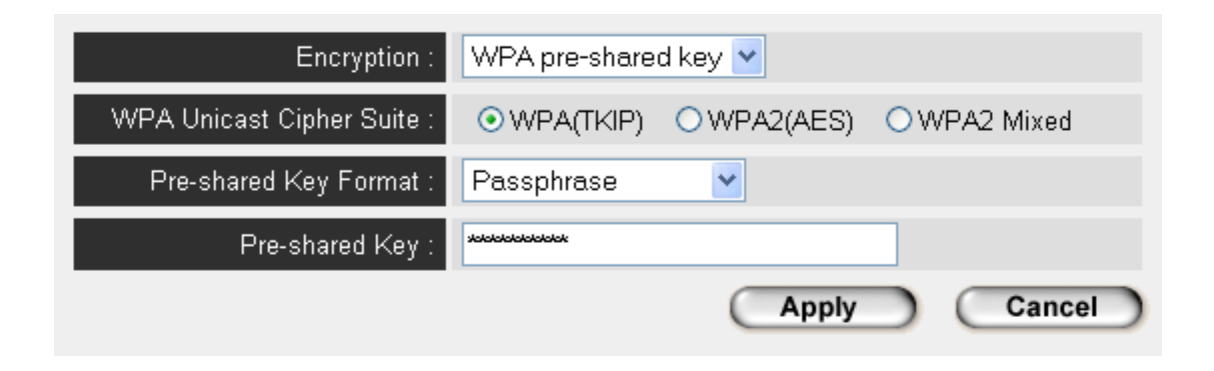


Wird diese Meldung angezeigt, wurden Ihre Einstellungen erfolgreich gespeichert. Klicken Sie auf „Continue” [Fortfahren], um zum vorherigen Einstellungsmenü zurückzukehren oder klicken Sie auf „Apply” [Übernehmen], um den Access Point neu zu starten. Der Neustart dauert ca. 30 Sekunden, danach wurden Ihre Änderungen übernommen.

2-7-3 WPA Pre-shared Key [vorher vereinbarter Schlüssel]

WPA Pre-shared key ist z. Z. die sicherste Verschlüsselungsmethode und es wird empfohlen, diese zu nutzen, um Ihre Datensicherheit zu erhöhen.

Wenn Sie “WPA pre-shared key” als Verschlüsselungsmethode auswählen, öffnet sich folgendes Fenster:

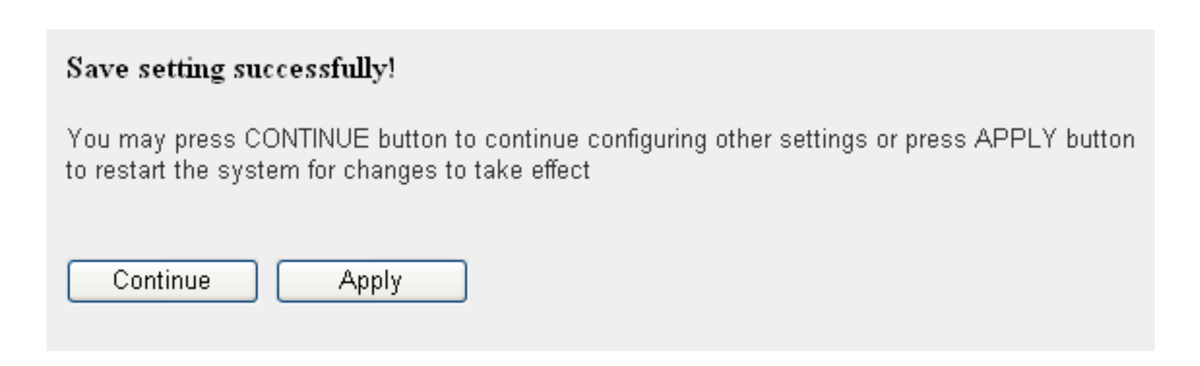


Die Optionen im Einzelnen:

WPA Unicast Cipher Suite	*Sie können zwischen verschiedenen WPA-Verschlüsselungen wählen. Verfügbar sind: WPA (TKIP), WPA2 (AES), und WPA2 Mixed. Achten Sie darauf, dass Ihr Wireless Client Ihre gewählte Verschlüsselungsart auch unterstützt.*
Pre-shared Key Format	*Wählen Sie den pre-shared key (vorher vereinbarter Schlüssel). Sie können wählen zwischen: Passphrase (8 oder mehr alphanumerische Zeichen, bis zu 63) oder Hex (64 Zeichen von 0-9 und a-f).*
Pre-shared Key	*Geben Sie den pre-shared key entsprechend Ihres gewählten Schlüsselformats ein. Verwenden Sie aus Sicherheitsgründen keine simplen Wörter.*

Haben Sie alle Einstellungen vorgenommen, klicken Sie auf „Ap-

ply" [Übernehmen], worauf folgende Meldung erscheint:

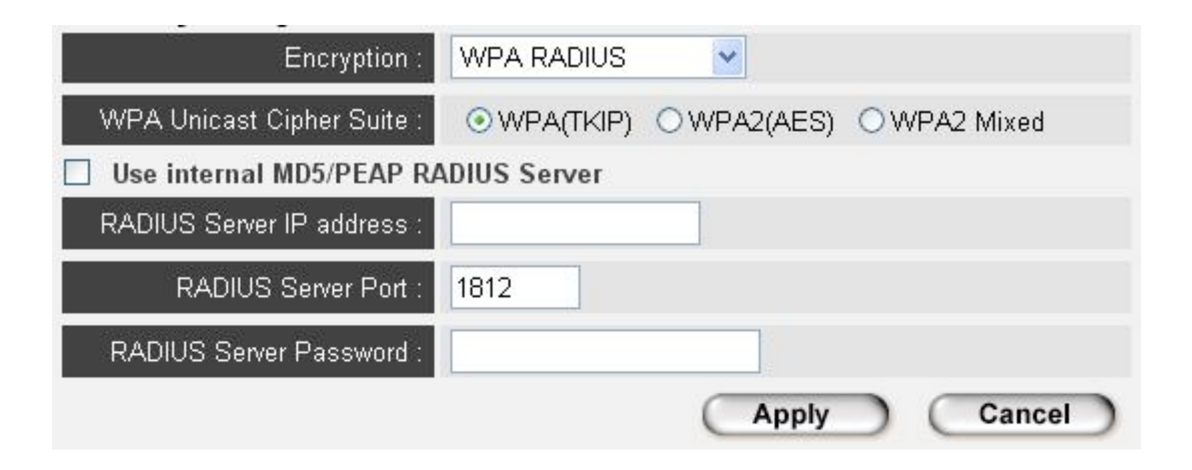


Wird diese Meldung angezeigt, wurden Ihre Einstellungen erfolgreich gespeichert. Klicken Sie auf „Continue" [Fortfahren], um zum vorherigen Einstellungsmenü zurückzukehren oder klicken Sie auf „Apply" [Übernehmen], um den Access Point neu zu starten. Der Neustart dauert ca. 30 Sekunden, danach wurden Ihre Änderungen übernommen.

2-7-4 WPA RADIUS

WPA RADIUS ist eine Kombination aus WPA-Verschlüsselungsmethode und RADIUS-Benutzerauthentifizierung. Verfügen Sie über einen RADIUS-Authentifizierungsserver, können Sie die Identität jedes Wireless Client mit einer Benutzerdatenbank abgleichen.

Wenn Sie “WPA RADIUS” als Verschlüsselungsart auswählen, wird folgende Meldung angezeigt:

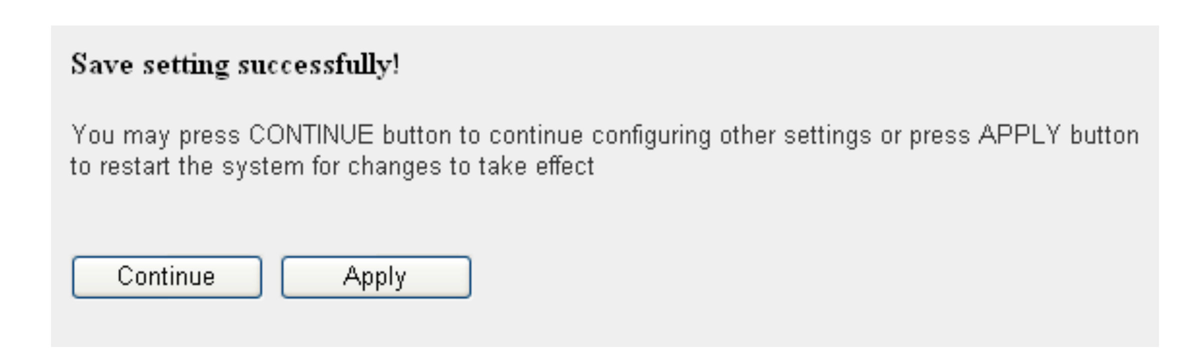


Die Optionen im Einzelnen:

WPA Unicast Cipher Suite	*Hier können Sie die WPA-Verschlüsselung auswählen. AES ist sicherer als TKIP, wird aber nicht von jedem Wireless Client unterstützt.Lesen Sie in den Spezifikationen, welche Verschlüsselungsart Sie verwenden sollten.*
Use internal MD5/PEAP RADIUS Server	*Nutzen Sie den integrierten RADIUS-Server (mehr dazu in Abschnitt 2-8) statt einem externen RADIUS-Server. Setzen Sie hier ein Häkchen, werden die Preise in den folgenden drei Feldern ignoriert.*
RADIUS Server IP address	*Geben Sie hier die IP-Adresse Ihres RADIUS- Authentifizierungsservers ein.*
RADIUS Server Port	*Geben Sie hier die Port-Nummer Ihres Radius Authentifizierungsservers ein.* ***Die Standardein-***

	stellung lautet 1812.
RADIUS Server Password	*Geben Sie hier das Passwort Ihres RADIUS-Authentifizierungsservers ein.*

Haben Sie alle Einstellungen vorgenommen, klicken Sie auf „Apply” [Übernehmen], worauf folgende Meldung erscheint:



Wird diese Meldung angezeigt, wurden Ihre Einstellungen erfolgreich gespeichert. Klicken Sie auf „Continue” [Fortfahren], um zum vorherigen Einstellungsmenü zurückzukehren oder klicken Sie auf „Apply” [Übernehmen], um den Access Point neu zu starten. Der Neustart dauert ca. 30 Sekunden, danach wurden Ihre Änderungen übernommen.

2-7-5 802.1x Authentifizierung

Sie können die 802.1x-Benutzeridentifikation (auf Basis des RADIUS Authentifizierungsservers) aktivieren, indem Sie bei „Enable 802.1x Authentication" ein Häkchen setzen, nachdem Sie „Disable" [Deaktivieren] oder "WEP" Verschlüsselungsart ausgewählt haben. Folgende Optionen werden angezeigt:

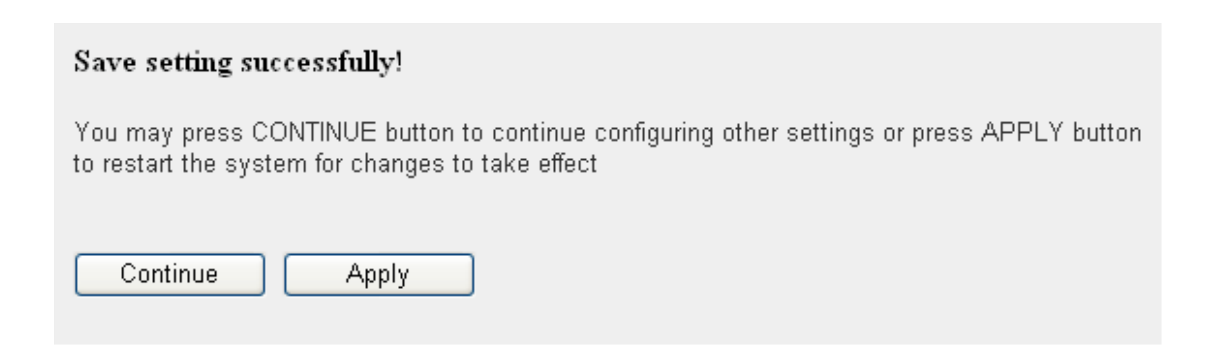


Die Optionen im Einzelnen:

Select SSID	*Wählen Sie die SSID aus, die Sie konfigurieren möchten.*
Use internal MD5/PEAP RADIUS Server	*Nutzen Sie den integrierten RADIUS-Server (siehe nächster Abschnitt) statt einem externen RADIUS-Server. Setzen Sie hier ein Häkchen, werden alle anderen RADIUS-Servereingabefelder ignoriert.*
Enable 802.1x Authentication	*Aktiviert oder deaktiviert die Anwendung von 802.1x-Benutzerauthentifizierung.*
RADIUS Server IP address	*Geben Sie hier die IP-Adresse des RADIUS-Authentifizierungsservers ein.*
RADIUS Server Port	*Geben Sie hier die Portnummer des RADIUS-Authenfizierungsservers ein. Der Standardwert lautet 1812.*
RADIUS Server	*Geben Sie hier das Passwort des RADI-*

Password	US-Authentifizierungsservers ein.

Haben Sie alle Einstellungen vorgenommen, klicken Sie auf „Apply” [Übernehmen], worauf folgende Meldung erscheint:



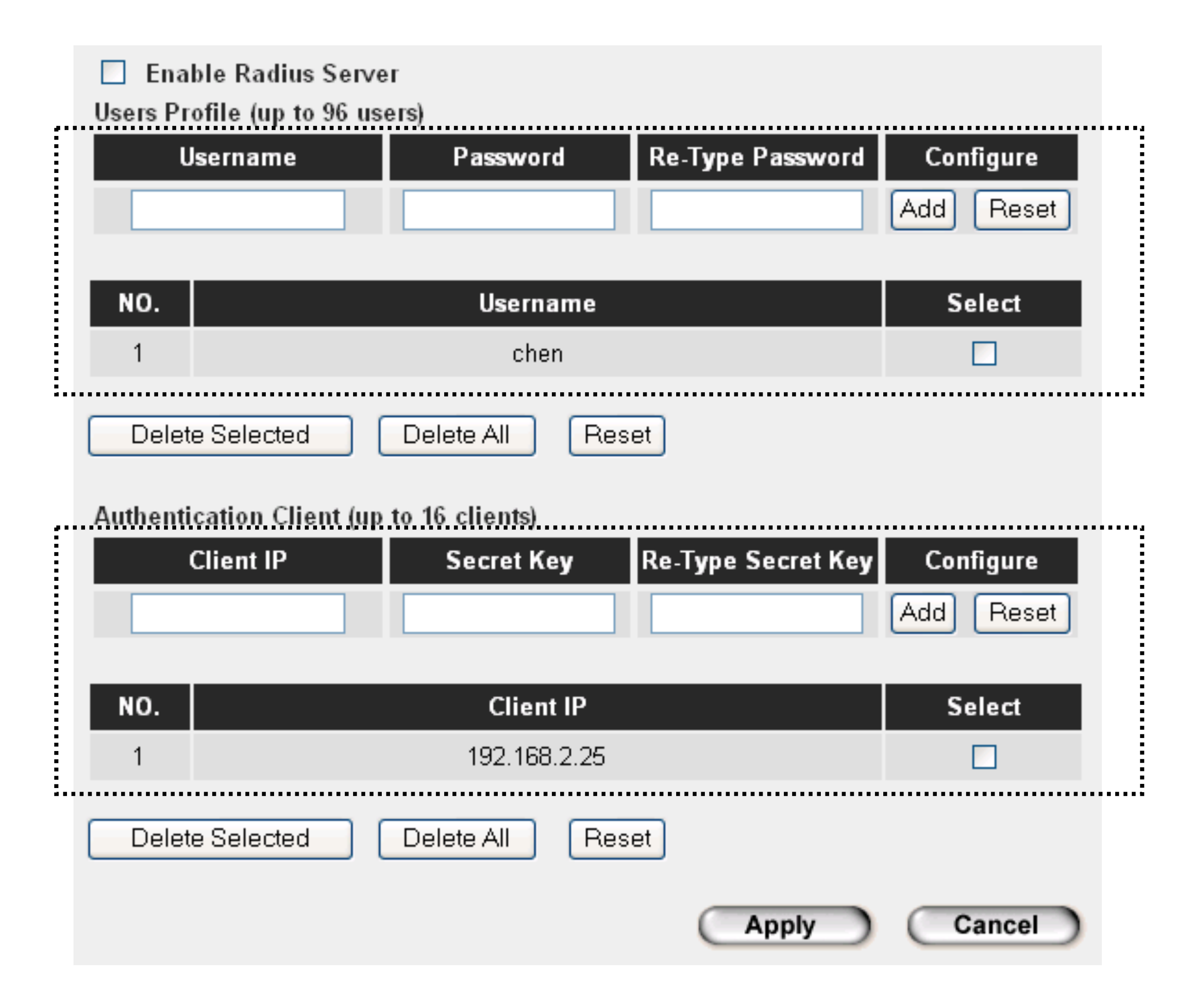
Wird diese Meldung angezeigt, wurden Ihre Einstellungen erfolgreich gespeichert. Klicken Sie auf „Continue” [Fortfahren], um zum vorherigen Einstellungsmenü zurückzukehren oder klicken Sie auf „Apply” [Übernehmen], um den Access Point neu zu starten. Der Neustart dauert ca. 30 Sekunden, danach wurden Ihre Änderungen übernommen.

2-8 RADIUS-Server

Im Vergleich mit anderen Wireless Sicherheitsmaßnahmen, bietet ein RADIUS-Server nutzerbasierte Authentifizierung. Wenn Ihr Wireless Client 802.1x Benutzerauthentifizierung unterstützt, können Sie die RADIUS-Serverfunktion nutzen, um mit dem internen Mini-RADIUS-Server die Sicherheit zu erhöhen und Wireless Benutzerkontrolle.

Der interne RADIUS-Server unterstützt nur 96 Nutzer und 16 IP-Adressen. Wenn Sie eine größere diese Zahl an Nutzern und/oder IP-Adressen haben, verwenden Sie einen externen RADIUS server.

Um den internen RADIUS-Server zu konfigurieren, klicken Sie in der Web-Benutzeroberfläche auf „RADIUS Server“ woraufhin folgendes Fenster geöffnet wird:

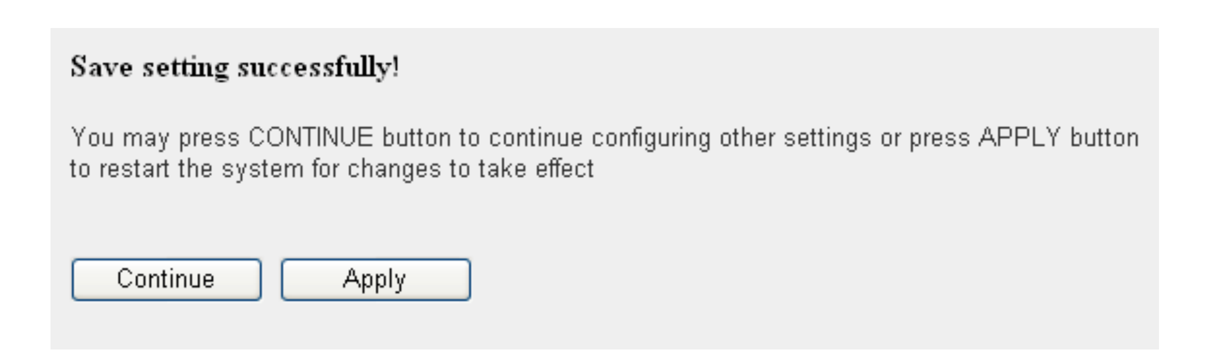


Die Optionen im Einzelnen:

Enable RADIUS Server	*Setzen Sie hier ein Häkchen, um die interne RADIUS-Serverfunktion zu aktivieren.*
User Profile	*Hier können Sie RADIUS-Nutzer hinzufügen oder entfernen. Geben Sie Benutzername und Passwort in den entsprechenden Feldern ein und klicken Sie auf „Add", um den Benutzer zur RADIUS-Serverdatenbank hinzuzufügen. Sie können auf „Reset" klicken, um Ihre Eingaben in den vorherigen drei Feldern zu löschen. Alle aktuellen RADIUS-Nutzer werden hier*

	aufgelistet. Um einen oder mehrere Nutzer zu entfernen, klicken Sie auf dessen „Se-lect-Kästchen“ und dann auf “Delete Selec-ted”. Klicken Sie auf „Delete All“, um alle Nut-zer in der RADIUS-Serverdatenbank zu ent-fernen.Sie können jederzeit auf „Reset“ klic-ken, um Ihre Auswahl aufzuheben.
Authentication Client	*Hier können Sie zugelassene RADIUS-Client-IP-Adressen eingeben. Geben Sie die Client IP ein und den Schlüssel in den entsprechen-den Feldern.Anschließend klicken Sie auf „Add”, um die IP-Adresse zur RADIUS Ser-verdatenbank hinzgefügt haben. Sie können auf „Reset“ klicken, um Ihre Eingaben in den vorherigen drei Feldern zu löschen.* *Alle aktuellen IP-Adressen werden hier aufge-listet. Möchten Sie eine oder mehrere Adres-sen entfernen, klicken Sie auf deren „Se-lect-Kästchen“ und dann auf “Delete Selec-ted”. Klicken Sie auf „Delete All“, um alle Adressen in der RADIUS-Serverdatenbank zu entfernen.Sie können jederzeit auf „Re-set“ klicken, um Ihre Auswahl aufzuheben.*

Haben Sie alle Einstellungen vorgenommen, klicken Sie auf „Ap-ply” [Übernehmen], worauf folgende Meldung erscheint:



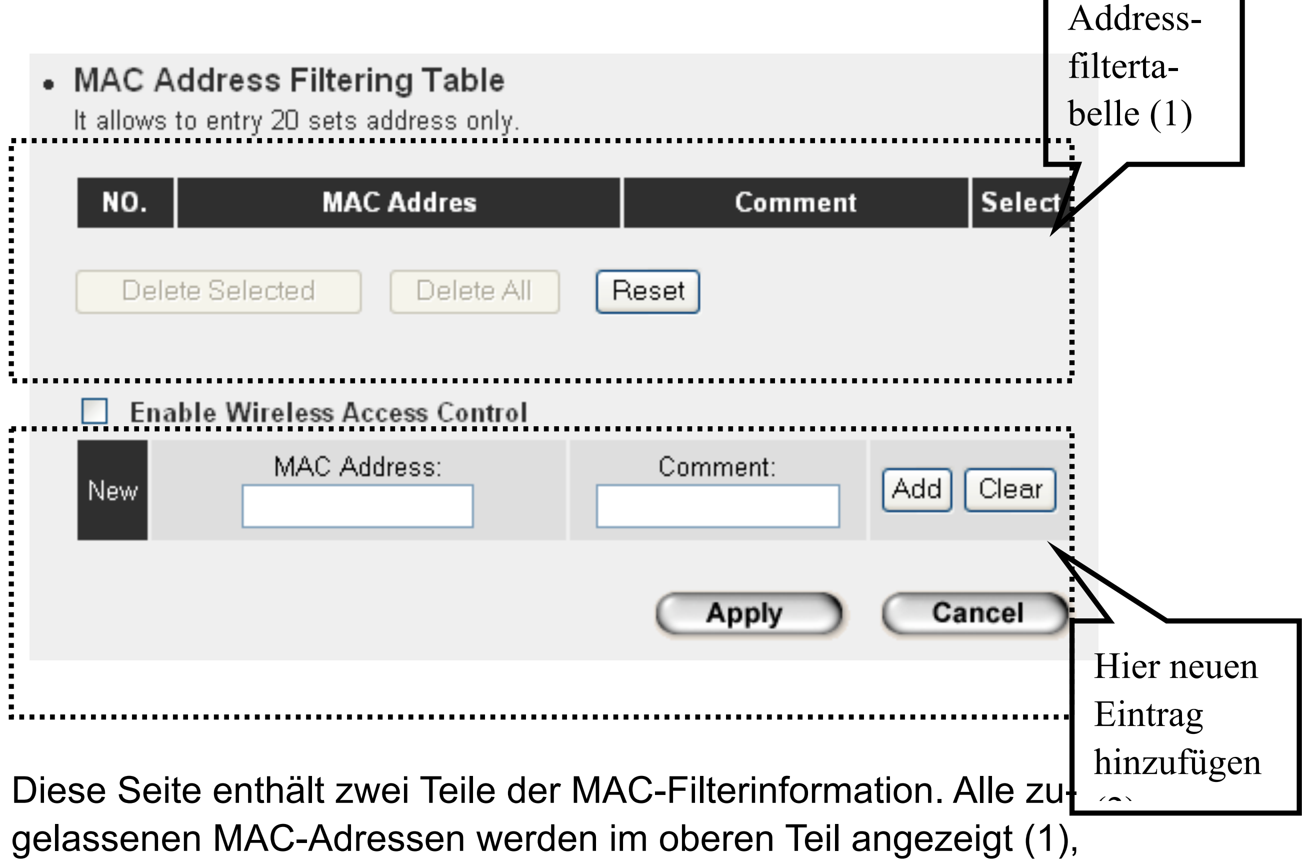
Wird diese Meldung angezeigt, wurden Ihre Einstellungen erfolg-reich gespeichert. Klicken Sie auf „Continue” [Fortfahren], um zum

vorherigen Einstellungsmenü zurückzukehren oder klicken Sie auf „Apply” [Übernehmen], um den Access Point neu zu starten. Der Neustart dauert ca. 30 Sekunden, danach wurden Ihre Änderungen übernommen.

2-9 MAC-Filterung

Eine weitere Sicherheitsmaßnahme gegen Hacker ist die MAC-Filterung. Sie können eine so genannte “White-List” erstellen, die MAC-Adressen von Wireless Clients auflistet, denen Sie vertrauen. Alle Wireless Clients mit MAC-Adressen, die nicht auf Ihrer Liste stehen, wird der Zugriff auf diesen Wireless Access Point verweigert.

Um die MAC-Filterung zu konfigurieren, klicken Sie auf „MAC Filtering“ auf der linken Seite der Web-Benutzeroberfläche, woraufhin folgende Meldung angezeigt wird:



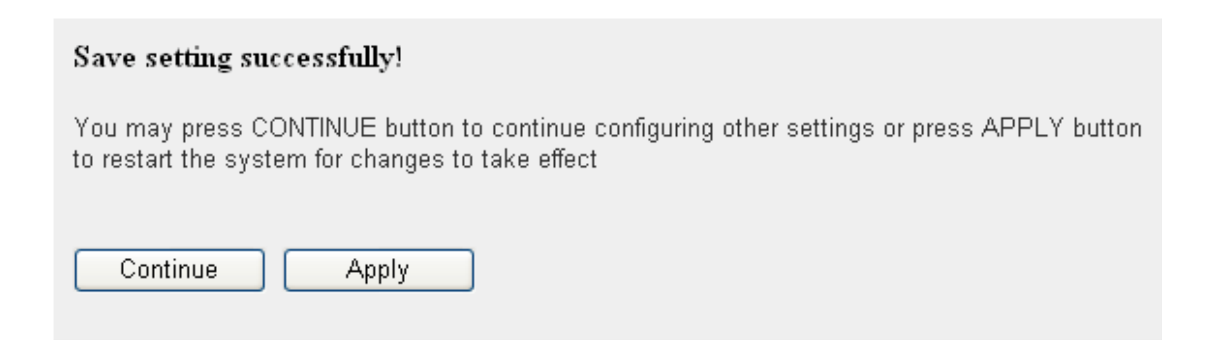
Diese Seite enthält zwei Teile der MAC-Filterinformation. Alle zugelassenen MAC-Adressen werden im oberen Teil angezeigt (1), und Sie können neue MAC-Adressen über die Komponenten im unteren Teil (2) eintragen.

Die Optionen im Einzelnen:

Select	*Setzen Sie ein Häkchen, um eine oder mehrere MAC-Adress zum Löschen auszuwählen.*
Delete Selected	*Klicken Sie, um alle ausgewählten*

	MAC-Adressen zu löschen.
Delete All	*Löscht alle MAC-Adresseneinträge.*
Reset	*Hebt die Auswahl MAC-Adressen wieder auf.*
Enable Wireless Access Control	*Setzen Sie ein Häkchen, um die MAC-Adresssperre zu aktivieren. Lassen Sie sie deaktiviert, kann sich jeder Wireless Client mit den korrekten Verschlüsselungseinstellungen mit diesem Wireless Access Point verbinden).*
MAC address	*Geben Sie hier eine MAC-Adresse ein, der Sie Zugang zu diesem Access Point gewähren möchten. Sie müssen Doppelpunkte (:) und Bindestriche (-) nicht selbst eingeben: Geben Sie hier einfach 0 bis 9 und a bis f ein; z. B., 112233445566 oder aabbccddeeff.*
Comment	*Sie können hier einen Kommentartext zu jeder MAC-Adresse eintragen, z. B. „Raum 2“. Sie können bis zu 16 alphanumerische Zeichen eintragen. Diese Eingaben sind optional, Sie können die Felder auch freilassen, allerdings wird das Ausfüllen empfohlen, um die Identifizierung der einzelnen MAC-Adressen zu erleichtern.*
Add	*Klicken Sie auf „Add“ [Hinzufügen], um MAC-Adressen und entsprechenden Kommentartexte zur MAC-Adressenfilterungsliste hinzuzufügen.*
Clear	*Klicken Sie auf „Clear“ [Löschen], um Ihre eingegebenen Werte in MAC-Adressen- und Kommentarfeld zu entfernen.*

Haben Sie alle Einstellungen vorgenommen, klicken Sie auf „Apply” [Übernehmen], worauf folgende Meldung erscheint:



Wird diese Meldung angezeigt, wurden Ihre Einstellungen erfolgreich gespeichert. Klicken Sie auf „Continue” [Fortfahren], um zum vorherigen Einstellungsmenü zurückzukehren oder klicken Sie auf „Apply” [Übernehmen], um den Access Point neu zu starten. Der Neustart dauert ca. 30 Sekunden, danach wurden Ihre Änderungen übernommen.

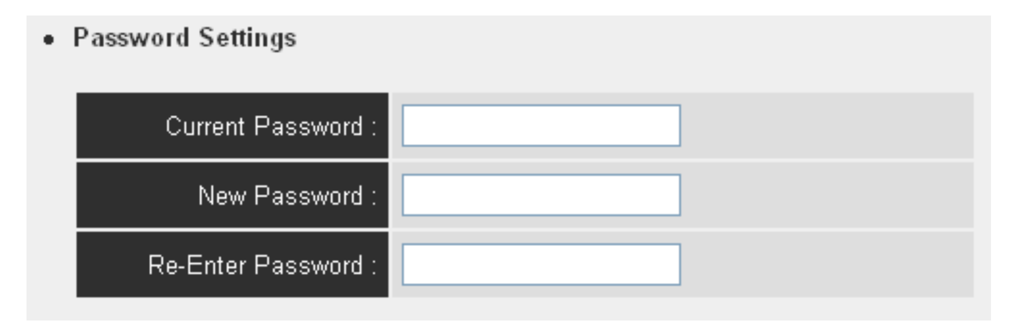
2-10 System Utilities

Dieser Access Point bietet Kontrollfunktionen, Passwort, IP-Adressenmanagement und DHCP-Serverfunktion. Klicken Sie auf „System Utility“ auf der linken Seite der Web-Benutzeroberfläche, um auf diese Funktionen zuzugreifen. Im Folgenden finden Sie genaue Beschreibungen jeder Funktion.

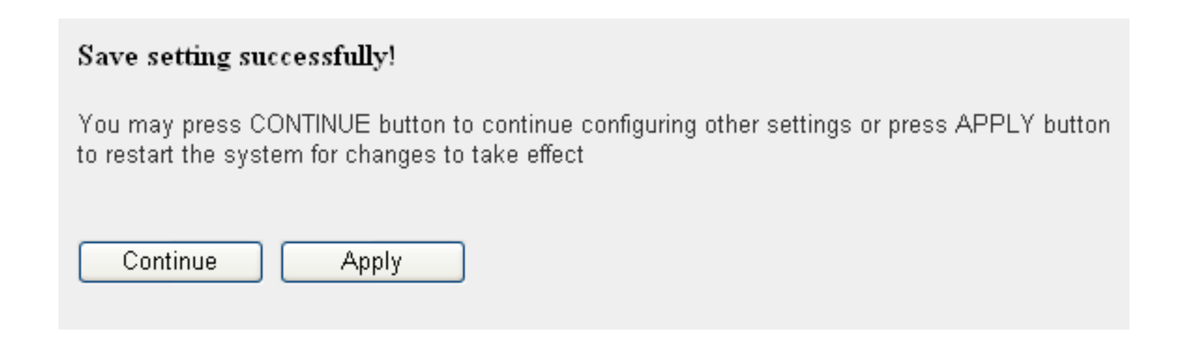
2-10-1 Passwort ändern

Sie können das Passwort ändern, das verwendet wird, um das Web-Einstellungmenü Wireless Access Point zuzugreifen.

Klicken Sie links auf „System Utility“, woraufhin folgendes Fenster geöffnet wird:



Geben Sie das aktuelle Passwort im Feld „Current Password“ ein, dann das neue Passwort sowohl in das Feld „New Password” [Neues Passwort] als auch in das Feld „Re-Enter Password” [Passwort erneut eingeben]. Klicken Sie auf „Apply”, woraufhin folgende Meldung angezeigt wird:



Wird diese Meldung angezeigt, wurden Ihre Einstellungen erfolgreich gespeichert. Klicken Sie auf „Continue” [Fortfahren], um zum

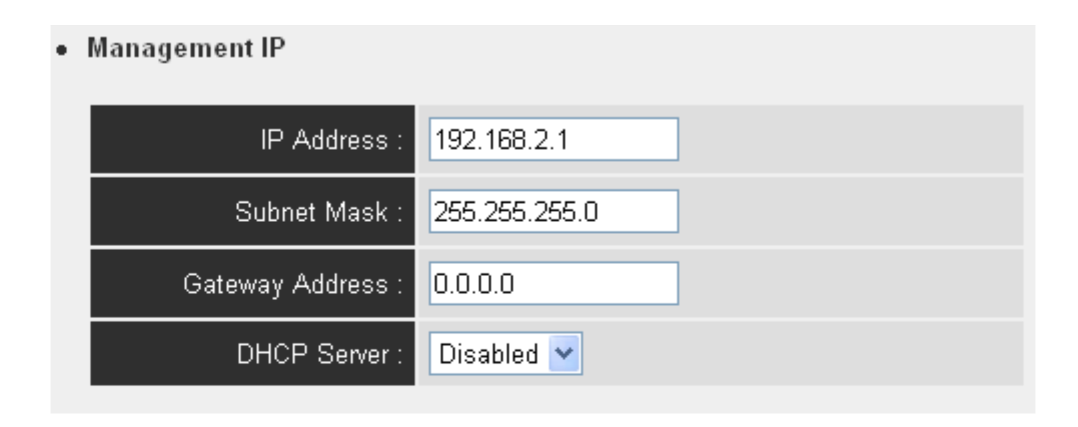
vorherigen Einstellungsmenü zurückzukehren oder klicken Sie auf „Apply” [Übernehmen], um den Access Point neu zu starten. Der Neustart dauert ca. 30 Sekunden, danach wurden Ihre Änderungen übernommen.

2-10-2 IP Address des Wireless Access Point

Sie können die IP-Adresse dieses Wireless Access Point ändern, damit Sie Teil Ihres lokalen Netzwerks wird. Merken Sie sich diese Adresse oder Sie werden nicht mehr in der Lage sein, sich im Konfigurationsmenü dieses Wireless Access Points einzuloggen.

Die Standard-IP-Adresse lautet 192.168.2.1; die Subnetzmaske 255.255.255.0. Halten Sie den Knopf „Reset/WPS” länger als 10 Sekunden gedrückt, um die IP-Adresse wieder auf den Standardwert zurückzusetzen, falls Sie sie vergessen haben.

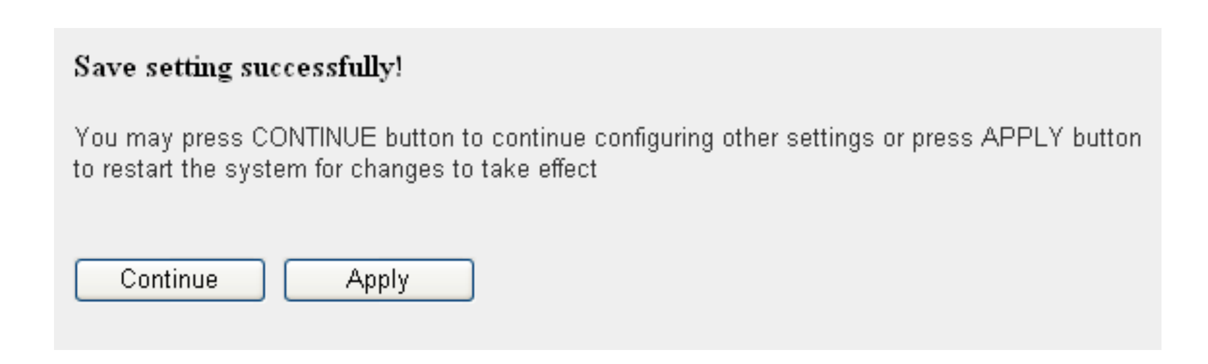
Um die IP-Adresse zu ändern, klicken Sie auf „System Utility“, woraufhin folgendes Fenster geöffnet wird:



Geben Sie die IP-Adresse und Subnetzmaske die entsprechenden Felder ein und die IP-Adresse des Gateways in das „Gateway Address”-Feld, wenn Sie diesen Wireless Access Point von einem anderen Netzwerk aus verwalten möchten (z. B. über das Internet).

Um die DHCP-Serverfunktion dieses Wireless Access Point zu aktivieren, wählen Sie „Enabled” bei der „DHCP Server”-Option aus. Im folgenden Abschnitt finden Sie detaillierte Anweisungen hierzu. Möchten Sie die DHCP-Serverfunktion dieses Access Points nicht verwenden oder falls ein anderer DHCP-Server im Netzwerk verfügbar ist wählen Sie „Disable” aus.

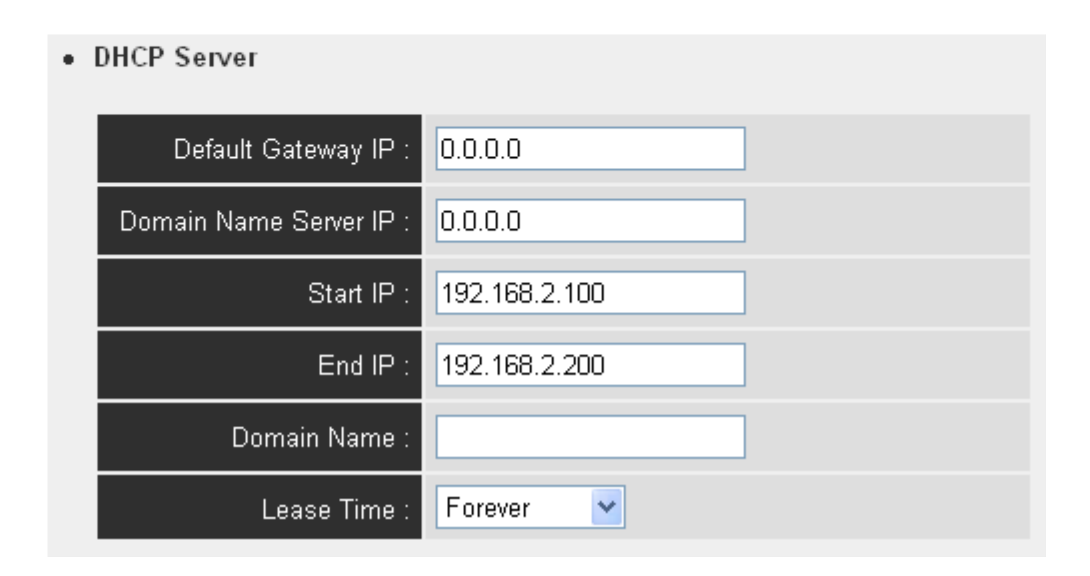
Klicken Sie auf „Apply” [Übernehmen], woraufhin folgende Meldung angezeigt wird:



Wird diese Meldung angezeigt, wurden Ihre Einstellungen erfolgreich gespeichert. Klicken Sie auf „Continue” [Fortfahren], um zum vorherigen Einstellungsmenü zurückzukehren oder klicken Sie auf „Apply” [Übernehmen], um den Access Point neu zu starten. Der Neustart dauert ca. 30 Sekunden, danach wurden Ihre Änderungen übernommen.

2-10-3 DHCP-Server

Dieser Wireless Access Point kann als DHCP-Server für Ihr Netzwerk fungieren, was standardmäßig deaktiviert ist. Möchten Sie diese Funktion deaktivieren, klicken Sie links auf System Utility, woraufhin folgendes Fenster geöffnet wird:



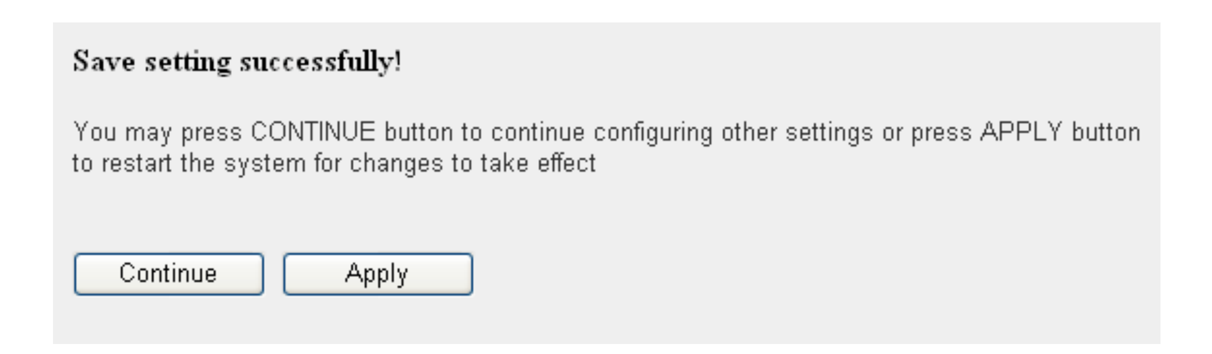
HINWEIS: Denken Sie daran, die „DHCP Server"-Option mit „Enabled" zu aktivieren, wie im letzten Abschnitt beschrieben, andernfalls bleiben alle DHCP-bezogenen Felder grau und Sie können dort keine Werte eingeben.

Die Optionen im Einzelnen:

Default Gateway IP	*Geben Sie hier die IP-Adresse des Standardgateways Ihres Netzwerks ein.*
Domain Name Server IP	*Geben Sie hier die IP-Adresse des Domain Name Servers (DNS) ein.*
Start IP	*Geben Sie hier die Start-IP des IP-Adressbereichs ein.*
End IP	*Geben Sie hier die End-IP des IP-Adressbereichs ein.*
Domain Name	*Auf Wunsch können Sie auch den Domain-Namen Ihres Netzwerks angeben. Dies ist optional.*
Lease Time	*Wählen Sie aus dem Drop-Down-Menü eine Lease*

	Time für jede IP-Adresse, die von diesem Access Point zugewiesen wurde. Die Lease Time bezeichnet den Zeitraum, für den jeder Computer eine bestimmte IP-Adresse behalten kann.

Klicken Sie auf „Apply” [Übernehmen], woraufhin folgende Meldung angezeigt wird:



Wird diese Meldung angezeigt, wurden Ihre Einstellungen erfolgreich gespeichert. Klicken Sie auf „Continue” [Fortfahren], um zum vorherigen Einstellungsmenü zurückzukehren oder klicken Sie auf „Apply” [Übernehmen], um den Access Point neu zu starten. Der Neustart dauert ca. 30 Sekunden, danach wurden Ihre Änderungen übernommen.

Abschnitt 3: Erweiterte Einstellungen

3-1 Archivierung und Wiederherstellung der Konfiguration

Sie können jede Konfigurationen dieses Access Points als Datei speichern. Aus Sicherheitsgründen können Sie auch problemlos mehrere Konfigurationsdateien anlegen.

Um Ihre Access-Point-Konfigurationen zu archivieren oder wiederherzustellen, folgen Sie diesen Anweisungen:

Klicken Sie auf „Configuration Tool“ auf der linken Seite der Web-Benutzeroberfläche, woraufhin folgendes Fenster geöffnet wird:

Backup Settings : Save...

Restore Settings : Browse... Upload

Restore to Factory Default : Reset

Die Optionen im Einzelnen:

Backup Settings	*Klicken Sie auf „Save...“ und wählen Sie einen Speicherort für die Datei. Der Standardname lautet „default.bin“. Speichern Sie unterschiedliche Versionen unterschiedlichen Namen und bewahren Sie sie in sicheren Ordnern auf.*
Restore Settings	*Klicken Sie auf „Browse…“ [Durchsuchen] um auf zuvor gespeicherte Einstellungen zuzugreifens (2): und dann auf „Upload“, um diese auf den Access Point zu übertragen. Die aktuelle Konfiguration des AP wird dann von Ihrer übertragenen Datei ersetzt.*
Restore to Factory Default	*Entfernen Sie vorgenommene Einstellungen und setzen Sie den Access Point auf die*

	Werkseinstellungen zurück.

3-2 Firmware-Aktualisierung

Wenn eine neue Firmware-Version für diesen Wireless Access Point verfügbar ist, können Sie diese auf das Gerät laden, für erweiterte Funktionen oder, um bestehende Probleme zu lösen.

Um eine Firmware-Aktualisierung durchzuführen, klicken Sie auf „Upgrade“ links auf der Web-Benutzeroberfläche, woraufhin sich folgendes Fenster öffnet:

Firmware Upgrade

This tool allows you to upgrade the Access Point's firmware. Firmware upgrades should only be performed with a computer that is connected to the Access Point via a network cable.
Enter the path and name of the upgrade file, then click APPLY. You will be prompted to confirm the upgrade.

Browse...

Klicken Sie zunächst auf „Browse” [Durchsuchen]: Sie werden nach dem Dateinamen der Firmwareaktualisierungsdatei gefragt. Nachdem Sie eine Firmware-Aktualisierungsdatei ausgewählt haben, klicken Sie auf „Apply” [Übernehmen], woraufhin der Access Point den Firmware-Aktualisierungsvorgang automatisch durchführt. Der Vorgang kann einige Min.

HINWEIS: Während des Aktualisierungsvorgangs sollten Sie auf keinen Fall den Browser schließen oder den Access Point vom Computer trennen. Ist die Firmware, die Sie geladen haben beschädigt, wird der Aktualisierungsvorgang fehlschlagen und Sie müssen sich an Ihren

3-3 Systemwiederherstellung

Haben Sie Grund zur Annahme, dass der Access Point nicht korrekt funktioniert, können Sie diese Funktion nutzen, um den Access Point neuzustarten, was das Problem evtl. löst.

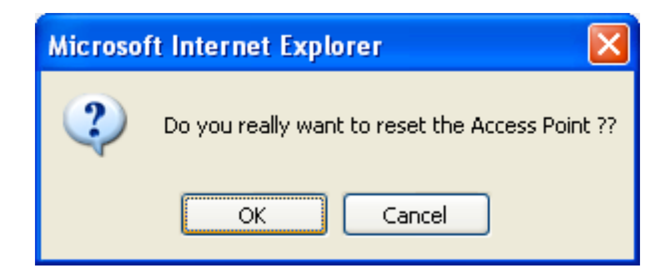
Diese Funktion ist nützlich, wenn sich der Access Point in der näheren Umgebung befindet. Sollte der Access Point nicht ansprechen, müssen Sie ihn kurz von der Stromversorgung trenne und nach etwa 10 Sekunden wieder anschließen.

Um einen Reset durchzuführen, klicken Sie links auf „Reset“. Folgende wird eingeblendet:

Restart

This screen allows you to perform a system restart. Click APPLY below to begin the process. You will be asked to confirm your decision. The restart is completed when the Power LED stops flashing.

Klicken Sie auf “Apply” [Übernehmen] woraufhin Sie gefragt werden, ob Sie den Reset wirklich durchführen möchten:



Klicken Sie auf “OK”, um den Access Point zurückzusetzen oder „Cancel”, um vorher abzubrechen. Denken Sie daran, dass alle bestehenden Verbindungen zwischen Wireless Clients und diesem Access Point getrennt werden.

Abschnitt 4: Problemlösungen

Sollte der Access Point nicht korrekt arbeiten oder nicht mehr reagieren, lesen Sie die folgenden Problemlösungsvorschläge. Manche Probleme können ohne Unterstützung innerhalb kürzester Zeit gelöst werden.

Problem	Lösung
Der Access Point reagiert nicht, wenn ich über den Browser auf ihn zugreifern möchte	a. Überprüfen Sie den Anschluss des Strom- und Netzwerkkabels an diesem Access Point. Alle Kabel sollten fest und sicher in den Buchsen sitzen. b. Sie müssen denselben IP-Adressbereich wie der Access Point verwenden. c. Verwenden Sie einen IP- oder MAC-Adressenfilter? Verbinden Sie sich probeweise von einem anderen Computer mit dem Access Point und prüfen Sie, ob dies funktioniert; falls nicht, führen Sie einen Hard Reset durch (drücken Sie den Reset-Knopf). d. Konfigurieren Sie Ihren Computer so, dass er eine IP-Adresse automatisch bezieht (DHCP) und prüfen Sie, ob er diese erhält. e. Tritt der Fehler nach einer Firmware-Aktualisierung auf, wenden Sie sich an Ihren Händler. f. Wenn alle oben genannten Lösungen fehlschlagen, wenden Sie sich an Ihren Händler.
Ich kann keine Verbindung zum Access Point herstellen	a. Ist Verschlüsselung aktiviert, überprüfen Sie die WEP- oder WPA-Zeichenfolgeneinstellungen Ihres Wireless Clients. b. Bringen Sie den Client näher an den AP heran.

	c. Trennen Sie den Access Point etwa 10 Sekunden lang von der Stromversorgung und schließen Sie ihn dann wieder an.
Mein Wireless Client kann den Access Point nicht identifizieren.	a. Ist „Broadcast ESSID“ auf „Off“ [Aus] gestellt? b. Sind alle drei Antennen korrekt ange bracht? c. Sind Sie zu weit von Ihrem Access Point entfernt? Verringern Sie die Entfernung. d. Bedenken Sie, dass Sie die ESSID Ihres Wireless Client manuell eingeben müssen, wenn „ESSID broadcast“ deaktiviert ist.
Downloads laufen sehr langsam brechen häufig ab	a. Führen Sie einen Reset durch. b. Prüfen Sie die Aktivitäten anderer Computer in Ihrem lokalen Netzwerk. Falls gerade jemand große Datenmengen überträgt, wirkt sich das auf die Geschwindigkeit aller verbundenen Computer aus. c. Ändern Sie die Channel-Nummer.
Ich kann mich auf der Benutzeroberfläche im Browser nicht einloggen: falsches Passwort	a. Prüfen Sie, ob Sie die IP-Adresse des Access Points korrekt eingegeben haben. b. Beim Passwort wird zwischen Groß- und Kleinschreibung unterschieden. Stellen Sie sicher, dass die Feststelltaste nicht aktiviert ist. c. Haben Sie Ihr Passwort vergessen, führen Sie einen Hard Reset durch.
Der Access Point wird sehr heiß	a. Dies ist keine Fehlfunktion, eine erhöhte Betriebstemperatur ist absolut normal. b. Sollten Sie befremdlichen Geruch oder Rauch am Access Point oder Netzteil wahrnehmen, trennen Sie die Stromverbindung (sofern gefahrlos möglich) und kontaktieren Sie Ihren Händler.

Abschnitt 5: Glossar

Access point: Ein Access Point ist ein „intelligentes“ Netzwerkgerät, das Datenpakete zwischen Netzwerken versendet, auf der Basis von Schichteninformationen wie IP-Adressen.

DHCP: Dynamic Host Configuration Protocol. Dieses Protokoll vergibt IP-Adressen an alle Computer in Ihrem Heim-Netzwerk.

DNS-Server IP-Adresse: DNS steht für Domain Name System. Diese erlaubt Internet-Servern einen Domainnamen (z. B. www.accesspoint.com) und mehr als eine IP-Adresse (z. B. 192.34.45.8). Ein DNS-Server speichert Internet-Server und die entsprechenden Domainnamen und IP-Adressen in einer Datenbank, so dass ein Nutzer nach der Eingabe der Adresse www.accesspoint.com zur richtigen IP-Adresse weitergeleitet wird. Die DNS-Server-IP-Adresse, die von den Computern in Ihrem Heim-Netzwerk genutzt wird, ist der Ort des DNS-Servers, den Ihr Internetprovider Ihnen zugewiesen hat.

DSL-Modem: DSL steht für für Digital Subscriber Line. Ein DSL-Modem nutzt Ihre vorhandene Telefonleitung, um Daten mit High Speed zu übertragen.

Ethernet: Ein Standard für Computernetzwerke. Ethernet-Netzwerke werden mit speziellen Kabeln und Hubs verbunden und übertragen Daten mit einer Geschwindigkeit bis zu 10/100 Millionen Bits pro Sekunde (Mbit/s).

Idle Timeout: Idle Timeout bezeichnet die automatische Trennung der Internetverbindung nach einer vorher festgelegten Zeitspanne, in der keine Online-Aktivität festgestellt wurde.

IP-Adresse und Netzwerk- (Subnetz-) Maske: IP steht für Internet Protocol. Eine IP-Adresse besteht aus einer Reihe von vier Zahlen, die durch Punkte getrennt werden. Sie identifiziert einen einzelnen Host in einem IP-Netwerk, z. B. 192.168.2.1. Sie besteht aus zwei Teilen: der IP-Netwerk-Adresse und der Host-Kennung.

Gateway-Adresse des Internetproviders: (siehe Internetprovider). Eine IP-Adresse für den Internet-Router, der sich beim Internetprovider befindet.

Internetprovider: Internetprovider versorgen Privat- und Geschäftskunden sowie andere Organisationen mit Internetzugängen.

LAN: Local Area Network (Lokales Netzwerk). Ein LAN ist eine Gruppe von Computern und Geräten, die auf relativ kleinen Raum (z. B. in einem Haus oder Büro) miteinander verbunden sind. Ihr Heim-Netzwerk wird als LAN bezeichnet.

MAC-Adresse: MAC steht für Media Access Control. Eine MAC-Adresse is die Hardware-Adresse jedes einzelnen Netzwerkadapters, die zur eindeutigen Identifizierung des Geräts mit Ethernetschnittstelle in einem Rechnernetz dient. Sie besteht aus zwei Teilen: 3 Bytes entssprechen der Hersteller-ID (für jeden Hersteller einzigartig), plus 3 Bytes, die oft für die Seriennummer jedes Produkts verwendet werden.

NAT: Network Address Translation. Dieser Prozess erlaubt es allen Computern in Ihrem Heim-Netzwerk sich eine IP-Adresse zu teilen. Dadurch müssen Sie keine weiteren IP-Adressen von Ihrem Internetprovider erwerben.

Port: Netzwerk-Clients (LAN-PC) nutzen Port-Nummern, um einzelne Netzwerkanwendungen/Protokolle unterscheiden zu können. In unten stehender Liste finden Sie eine Reihe gebräuchlicher Anwendungen und Protokoll-/Port-Nummern:

Application	Protocol	Port Number
Telnet	TCP	23
FTP	TCP	21
SMTP	TCP	25
POP3	TCP	110
H.323	TCP	1720
SNMP	UCP	161
SNMP Trap	UDP	162
HTTP	TCP	80
PPTP	TCP	1723

PC Anywhere	TCP	5631
PC Anywhere	UDP	5632

PPPoE: Point-to-Point Protocol over Ethernet. Point-to-Point Protocol ist eine sichere Datenübertragungstechnik, die ursprünglich für Dial-up-Verbindungen verwendet wurden; PPPoE wird für Ethernet-Anschlüsse verwendet. PPPoE basiert auf zwei sehr verbreiteten Standards: Ethernet und Point-to-Point Protocol. Als Kommunikationsprotokoll überträgt es Informationen über Ethernet.

Protocol: Ein Protokoll ist eine Vereinbarung zur Interaktion zwischen mehreren Computern, damit diese Interaktion objektiv und genau definiert ist.

Standardgateway (Access Point): Alle Geräte außer dem Access Point benötigen eine Standardgateway-IP-Adresse. Wenn das Gerät ein IP-Datenpaket sendet, dessen Ziel sich nicht im selben Netzwerk befindet, muss das Gerät das Paket an seinen Standardgateway senden, der es dann an das Ziel weiterleitet.

Subnetzmaske: Eine Subnetzmaske, evtl. Teil der TCP/IP-Informationen Ihres Internetproviders, ist eine Reihe aus vier Zahlen (z. B. 255.255.255.0), die wie eine IP-Adresse konfiguriert sein kann. Sie wird verwendet, um IP-Adressen für bestimmte Netzwerke zu erstellen.

TCP/IP, UDP: Transmission Control Protocol/Internet Protocol (TCP/IP) und Unreliable Datagram Protocol (UDP). TCP/IP ist das Standard-Protokoll für Datenübertragungen über das Internet. Sowohl TCP als auch UDP sind Transportschichtprotokolle. TCP findet und behebt Fehler und ist daher „zuverlässig“. UDP dagegen ist „nicht zuverlässig“. Sie basieren beide auf IP (Internet Protocol), einem Netzwerkschichtprotokoll.

WAN: Wide Area Network. Ein Netzwerk, das Rechner in unterschiedlichen geographischen Lagen verbindet (z. B. in verschiedenen Gebäuden, Städten, Ländern). Das Internet ist beispielsweise ein Wide Area Network.

Web-Benutzeroberfläche: Viele Geräte unterstützen eine grafische Benutzeroberfläche direkt im Internetbrowser. Das bedeutet, der Benutzer kann

Einstellungen am Gerät auf der vertrauten Oberfläche des Firefox oder Microsoft Internet Explorers vornehmen.

Abschnitt 6: Spezifikationen

Standards
- IEEE 802.1d (Spanning Tree Protocol)
- IEEE 802.11b (11 Mbit/s Wireless LAN)
- IEEE 802.11g (54 Mbit/s Wireless LAN)
- IEEE 802.11n Draft 2.0 (300 Mbit/s Wireless LAN)
- IEEE 802.1x (Network Access Control)
- IEEE 802.3 (10Base-T Ethernet)
- IEEE 802.3u (100Base-TX Fast Ethernet)
- IEEE 802.3af (Power over Ethernet)

Allgemein
- LAN-Port: 1 RJ45 10/100 Mbit/s Daten- und Stromanschluss (PD-Port)
- Flash: 8 MB
- Speicher: 32 MB SDRAM
- Zertifikate: FCC Class B, CE, RoHS

Wireless
- Chipsatz: Ralink RT3052
- Wireless Reichweite: 2.400 – 2.483 GHz
- Modulationstechnologien:
  - 802.11b: Direct Sequence Spread Spectrum (DSSS): DBPSK, DQPSK, CCK
  - 802.11g: Orthogonal Frequency Division Multiplexing (OFDM): BPSK, QPSK, 16QAM, 64QAM
  - 802.11n: Orthogonal Frequency Division Multiplexing (OFDM): BPSK, QPSK, 16QAM, 64QAM
- Datenraten:
  - IEEE 802.11b (11 Mbit/s, 5.5 Mbit/s, 2 Mbit/s, 1 Mbit/s)
  - IEEE 802.11g (54 Mbit/s, 48 Mbit/s, 36 Mbit/s, 24 Mbit/s, 18 Mbit/s, 12 Mbit/s, 9 Mbit/s, 6 Mbit/s)
  - IEEE 802.11n (MCS0-15: bis zu 300 Mbit/s)
- Ausgangsleistung:
  - OFDM: 14 ± 1.5 dBm (300 Mbit/s, 40 mW max.)
  - OFDM: 15 ± 1.5 dBm (54 Mbit/s, 40 mW max.)
  - CCK: 17 ± 1.5 dBm (11 Mbit/s, 63 mW max.)

• Empfängerempfindlichkeit:
  - 11n (300 Mbit/s) ODFM: -68 ± 2 dBm
  - 11g (54 Mbit/s) OFDM: -74 ± 2 dBm
  - 11b (11 Mbit/s) CCK: -87 ± 2 dBm
• Wireless Betriebsmodi:
  - Access Point
  - Station Infrastructure (AP Client)
  - Point-to-Point Bridge
  - Point-to-Multi-Point Bridge
  - WDS Bridge
  - Universal Repeater
• Wireless Sicherheit:
  - WEP-Verschlüsselung (64/128 bit)
  - WPA TKIP
  - WPA2 AES
  - WPA2 mixed
  - WPA RADIUS
  - 802.1x Authentifizierung
  - Interner MD5/PEAP RADIUS Server
  - Client-Zugangskontrolle über Media Access Control (MAC) Filter
• Antennen:
  - 2 abnehmbare Dipolantennen mit jeweils 5 dBi Signalverstärkung pro Antenne, Typ-N-Anschluss
  - 2T2R-MIMO-Modus (2 Sender, 2 Empfänger)

Umgebung
• Abmessungen: 88 x 134 x 176 mm
• Gewicht: 2,3 kg
• Betriebstemperatur: -20 – 70°C
• Luftfeuchtigkeit: 10 – 90% RH, nicht-kondensierend
• Lagertemperatur: -40 – 80°C

Stromversorgung
• Netzteil: 48 V DC, 0,5 A (PoE)
• Leistungsaufnahme: 3,5 Watt max.
• Über PoE PD-Port: 48 V, 0,35 A



INTELLINET NETWORK SOLUTIONS® bietet ein vollständiges Sortiment aktiver und passiver Netzwerkkomponenten. Für weitere Informationen wenden Sie sich bitte an Ihren Händler oder nutzen Sie die Webseite

www.intellinet-network.com